
PROPERTY OF THE
University of
Michigan
Libraries
1817
ARTES SCIENTIA VERITAS

THEORIE

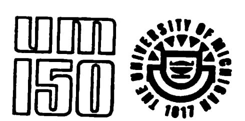
DER

ALGEBRAISCHEN GLEICHUNGEN

VON

Dr. JUL. PETERSEN

DOCENT AN DER POLYTECHNISCHEN SCHULE





Kommissionäre d. kgl. dän. Gesellschaft der Wissenschaften

1878



THEORIE

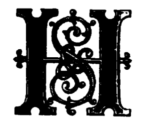
DER

ALGEBRAISCHEN GLEICHUNGEN

VON

Dr. JUL. PETERSEN

DOCENT AN DER POLYTECHNISCHEN SCHULE
IN KOPENHAGEN



KOPENHAGEN

ANDR. FRED. HÖST & SOHN

Universitätsbuchhändler

Kommissionäre d. kgl. dän. Gesellschaft der Wissenschaften

1878

GEDRUCKT BEI SALLY B. SALOMON.

VORWORT.

Dieses Buch verdankt seine Entstehung den Vorlesungen, welche ich an der polytechnischen Schule in Kopenhagen über die Theorie der Gleichungen gehalten habe. Durch Hinzufügung einiger erweiternder Zusätze habe ich versucht das Buch als einleitendes Studium für solche Studirende brauchbar zu machen, welche tiefer in die Wissenschaft der Algebra einzudringen wünschen.

Bei der Ausarbeitung habe ich namentlich J. A. Serret, Cours d'algèbre supérieure benutzt; an einzelnen Stellen ist Todhunter, Theory of equations benutzt, und von den Sätzen in der Theorie der Substitutionen sind viele aus Jordan, Traité des substitutions entnommen.

Viele Sätze, Methoden und Beweise sind in einer Form dargestellt, welche von der herkömmlichen nicht unerheblich abweicht. Wo Namen angeführt sind, sind diese deshalb oft nur so zu verstehen, dass die Entwicklung auf einer Idee aufgebaut

ist, ähnlich derjenigen, welche der Entwicklung des genannten Autors zu Grunde liegt.

Bekanntschaft mit den Anfangsgründen der Differentialrechnung ist für den Leser erwünscht; doch wird derjenige, welcher Taylor's Rechenentwicklung für ganze Functionen kennt, nur einige kleinere Abschnitte, die für das Ganze ohne wesentliche Bedeutung sind, zu überschlagen nöthig haben.

Kopenhagen, im Juni 1878.

Julius Petersen.

INHALT.

ERSTER ABSCHNITT.

UEBER GLEICHUNGEN IM ALLGEMEINEN.

Erstes Kapitel.

Zweites Kapitel.

Drittes Kapitel.

Viertes Kapitel.

ZWEITER ABSCHNITT.

UEBER DIE ALGEBRAISCHE AUFLOESUNG DER GLEICHUNGEN.

Erstes Kapitel.

Seite

Zweites Kapitel.

Drittes Kapitel.

Viertes Kapitel.

Fünftes Kapitel.

Sechtes Kapitel.

Siebentes Kapitel.

DRITTER ABSCHNITT.

UEBER DIE NUMERISCHE AUFLOESUNG DER GLEICHUNGEN.

Erstes Kapitel.

Drittes Kapitel.

Viertes Kapitel.

ERSTER ABSCHNITT.

UEBER GLEICHUNGEN IM ALLGEMEINEN.

Erstes Kapitel.

Allgemeine Eigenschaften der algebraischen Gleichungen.

Ueber complexe Ausdrücke.

1. Bezeichnet man den imaginären Ausdruck $\sqrt{-1}$ mit i, so wird die allgemeine Form für eine imaginäre Grösse, eine complexe Zahl,

$$a + bi,$$

worin a und b reell sind. Setzt man

$$a = r\cos\theta;\ b = r\sin\theta, \qquad (1)$$

so wird

$$a + bi = r(\cos\theta + i\sin\theta) \qquad (2)$$

und es ist

$$r = \sqrt{a^2 + b^2};\ \operatorname{tg}\theta = \frac{b}{a} \qquad (3)$$

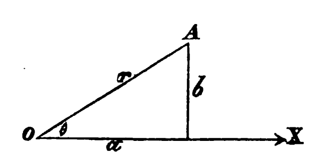
r heisst der *Modulus* der Grössen und wird *immer positiv* genommen; θ heisst das *Argument* und hat nur einen Werth zwischen 0 und 2π. (3) würde für θ allerdings 2 Werthe geben, aber (1) zeigt, dass $\cos\theta$ dasselbe Vorzeichen haben muss wie a, $\sin\theta$ dasselbe wie b; da aber die Vorzeichen

von cos und sin den Quadranten bestimmen, in welchem θ zu nehmen ist, so ist dadurch von den beiden zu $\operatorname{tg}\theta$ gehörigen Winkeln derjenige bestimmt, welcher gebraucht werden soll. In Wirklichkeit hat θ freilich unendlich viele Werthe, indem man $2p\pi$ (worin p eine beliebige ganze, positive oder negative Zahl bedeutet) zu dem gefundenen Winkel hinzu addiren kann; dieser Addend soll in der Folge jedesmal hinzugedacht werden, wo er keine Veranlassung zu Missverständnissen geben kann. Der Kürze wegen bezeichnet man auch die Grösse mit dem Modulus r und dem Argument θ mit r_θ.

Beispiel:

$$-1 = 1_\pi;\ i = 1_{\frac{\pi}{2}};\ -i = 1_{\frac{3\pi}{2}};\ -1 + i\sqrt{3} = 2_{\frac{2\pi}{3}};\ -1 - i\sqrt{3} = 2_{\frac{4\pi}{3}}.$$

2. Die complexe Grösse $a + bi$ kann durch einen Punkt geometrisch dargestellt werden. Hat man einen Anfangspunkt O und eine Anfangsrichtung X gewählt, so wird ein Punkt A dadurch bestimmt, dass man die Strecke r in der durch θ bestimmten Richtung abträgt, und diesen Punkt bezeichnet man dann mit r_θ. Man



sieht, dass diese Bestimmung mit der gewöhnlichen zusammenfällt, wenn der Punkt auf der X-Axe liegt. Hierdurch wird man darauf geführt, r als den numerischen Werth der Grösse aufzufassen, während der Factor $\cos\theta + i\sin\theta$, indem er die Richtung bestimmt, in welcher r abgetragen wird, die Rolle eines Vorzeichens spielt. Würde man $\sqrt{-}$ anstatt $\sqrt{-1}$ schreiben, so hätte man dadurch das neue Vorzeichen gewonnen, welches fehlt, um die Quadratwurzel aus einer negativen Zahl zu ziehen; während + und — zwei Richtungen auf der X-Axe bestimmen, bezeichnen $+i$ und $-i$ die beiden darauf senkrechten Richtungen. Es soll gleich gezeigt werden, wie mittelst einer passenden Erweiterung des

Begriffs der Addition durch diese Hauptrichtungen alle übrigen Richtungen bestimmt werden können.

Anstatt zu sagen, die complexe Grösse bezeichne den Punkt A, kann man auch sagen, dass sie die Strecke OA ihrer Richtung und Grösse nach ausdrückt.

Die beiden complexen Grössen $a + bi$ und $a - bi$ heissen *conjugirt;* sie haben denselben Modulus und ihre Argumente sind gleich gross, haben aber entgegengesetzte Vorzeichen. Die entsprechenden Punkte liegen symmetrisch zur X-Axe.

3. *Das Rechnen mit complexen Ausdrücken.* Der Begriff der Addition soll nun in der Art erweitert werden, dass man nach den gewöhnlichen Regeln mit complexen Ausdrücken rechnen kann; es sei also gegeben:

$$(a + b\,i) + (a_1 + b_1\,i) = (a + a_1) + (b + b_1)\,i.$$

Die beiden den Summanden entsprechenden Punkte haben die Coordinaten a, b und a_1; b_1, während der durch die Summe dargestellte Punkt die Coordinaten $a + a_1$ und $b + b_1$ hat. Die 3 durch diese Coordinaten bestimmten Punkte bilden mit dem Anfangspunkte die Eckpunkte eines Parallelogramms, dessen Seiten r und r_1 in den durch θ und θ_1 bestimmten Richtungen liegen. *Die Addition stellt also eine Parallelverschiebung dar, deren Grösse und Richtung durch den Modulus und das Argument des Addenden bestimmt wird.* Man sieht hier gleich die geometrische Bedeutung des Satzes, dass die Reihenfolge der Summanden beliebig ist.

Ist die Summe mehrerer complexer Grössen gleich Null, so kommt man durch die entsprechenden Verschiebungen zuletzt zum Anfangspunkt zurück und es wird ein geschlossenes Polygon gebildet; man kann deshalb sagen, dass die Summe der Seiten eines geschlossenen Polygons gleich Null sei, wenn man jede Seite mit einer complexen Zahl bezeichnet, die sowohl die Grösse als auch die Richtung derselben bestimmt, und wenn der Perimeter des Polygons in einer gewissen bestimmten Umlaufsrichtung durchlaufen wird. Dasselbe kann auch in der Form gesagt werden, dass ein Punkt auf dieselbe Weise ausgedrückt wird, einerlei auf welchem Wege man zu ihm gelangt. Auf diese Weise bedeutet (2),

dass man denselben Punkt erreicht, gleichgültig ob man die Strecke r in der durch θ bestimmten Richtung durchläuft, oder erst a in der Richtung + und dann b in der Richtung i. Hieraus folgt zugleich, *dass der Modulus einer Summe kleiner ist als die Summe der Moduln der Summanden,* vorausgestzt, dass nicht alle dasselbe Argument haben; ist das letztere der Fall, so ist der Modulus der Summe gleich der Summe der Moduln der Summanden.

Subtraction ist Addition mit entgegengesetzter Richtung.

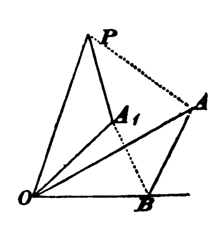
Der Begriff *der Multiplication* wird bestimmt durch

$$r(\cos\theta + i\sin\theta) . r_1(\cos\theta_1 + i\sin\theta_1) = r . r_1\left(\cos(\theta+\theta_1) + i\sin(\theta+\theta_1)\right)$$

oder

$$r_\theta . r_{1\theta_1} = (r r_1)_{\theta+\theta_1} . \qquad (4)$$

Wie man sieht, ist *der Modulus des Productes gleich dem Producte der Moduln der Factoren, während das Argument desselben gleich ist der Summe der Argumente der Factoren.* Ein hinzutretender Factor bewirkt also ausser einer Multiplication mit seinem Modulus im gewönlichen Sinne zugleich eine *Drehung,* die durch sein Argument bestimmt wird. Seien A und A_1 die beiden den Factoren entsprechenden Punkte, der Punkt B entspreche + 1 und P dem Producte. Es ergiebt sich dann leicht, dass $\Delta OBA \sim \Delta OA_1P$. Also ist das aus dem Producte und dem einen Factor gebildete Dreieck ähnlich dem aus dem anderen Factor und der Einheit gebildeten; *das Product ist aus dem einen Factor nach demselben Gesetze gebildet, nach welchem der andere Factor aus der Einheit gebildet ist.*



Man sieht, dass man auch zwei ähnliche Dreiecke erhält, wenn man A und A_1 vertauscht; hierin liegt die geometrische Bedeutung der Vertauschbarkeit der Factoren.

Beisp.

$$(-1)(-2) = 1_\pi 2_\pi = 2_{2\pi} = 2;\ i^2 = 1_{\frac{\pi}{2}} . 1_{\frac{\pi}{2}} = 1_\pi = -1.$$

Die *Division* wird auf die Multiplication zurückgeführt.

Für das *Potenziren* und *Radiciren* mit ganzen Exponenten erhält man nun

$$\left.\begin{aligned} (r_\theta)^n &= r^n{}_{n\theta} \\ \sqrt[n]{r_\theta} &= \left(\sqrt[n]{r}\right)_{\frac{\theta}{n}} \end{aligned}\right\} \quad \ldots\ldots\ldots\ldots \quad (5)$$

In der letzten Formel erhält das unter θ mitzuverstehende Glied $2p\pi$ Bedeutung, da verschiedene Werthe von p verschiedene Lösungen geben können. Es sollen in der Folge jedesmal gebrochene Exponenten angewendet werden, wenn es sich um alle Werthe einer Wurzelgrösse handelt, hingegen das Wurzelzeichen, wenn nur ein einzelner Werth bezeichnet werden soll; dann ist also

$$(r_\theta)^{\frac{1}{n}} = \left(\sqrt[n]{r}\right)_{\frac{2p\pi+\theta}{n}}, \quad \ldots\ldots\ldots\ldots \quad (6)$$

worin p die Werthe $0, 1 \ldots (n-1)$ durchlaufen kann. Für $p = n$ erhält man dasselbe Resultat wie für $p = 0$, für $p = n + \alpha$ dasselbe wie für $p = \alpha$. Die Anzahl der wirklich verschiedenen Werthe ist also n, und da die Richtungen dieser die ganze Umdrehung in n gleiche Theile theilen, die durch

$$\frac{\theta}{n}, \; \frac{\theta}{n} + \frac{2\pi}{n}, \; \frac{\theta}{n} + 2 \cdot \frac{2\pi}{n}, \ldots\ldots$$

bestimmt sind, so sind höchstens 2 der Werthe reell; reelle Werthe erhält man nämlich nur für

$$\frac{2p\pi+\theta}{n} = 0 \text{ oder für } \frac{2p\pi+\theta}{n} = \pi;$$

im ersten Falle muss $\theta = 0$ und $p = 0$ sein; im 2ten Falle $\theta = 0$ und $2p = n$, oder $\theta = \pi$ und $2p + 1 = n$. Ist die gegebene Grösse complex, so werden auch alle ihre Wurzeln complex; ist sie positiv, so wird eine Wurzel positiv und eine negativ, wenn n gerade ist, eine positiv, wenn n ungerade ist. Ist sie negativ, so wird eine Wurzel negativ,

wenn n ungerade ist; ist aber n gerade, so werden sie alle complex.

Durch Combination der bewiesenen Sätze ergiebt sich nun leicht, dass die Sätze über das Potenziren auch für gebrochene oder negative Exponenten gelten:

$$\left(r_\theta\right)^{-n} = \frac{1}{\left(r_\theta\right)^n} = \frac{1}{r^n_{n\theta}} = \left(r^{-n}\right)_{-n\theta},$$

$$\left(r_\theta\right)^{\frac{s}{q}} = \left(\left(r_\theta\right)^{\frac{1}{q}}\right)^s = \left(\sqrt[q]{r^s}\right)_{\frac{s}{q}(\theta + 2p\pi)}.$$

Lässt sich der Bruch $\frac{s}{q}$ verkürzen, so erhält man, wie leicht ersichtlich, weniger Auflösungen, wenn die Verkürzung ausgeführt wird.

Beisp. 1.

$$\left(\frac{-1 + i\sqrt{3}}{2}\right)^{\frac{1}{3}};\ r = 1;\ \theta = \frac{2\pi}{3}.$$

Die 3 Werthe sind also:

$$\cos 40^0 + i \sin 40^0;\ \cos 160^0 + i \sin 160^0;\ \cos 280^0 + i \sin 280^0.$$

Beisp. 2.

$$(-8)^{\frac{1}{3}};\ r = 8;\ \sqrt[3]{r} = 2;\ \theta = \pi;$$

Die Werthe sind also:

$$2_{\frac{\pi}{3}};\ 2_\pi \text{ und } 2_{\frac{5\pi}{3}} \text{ oder } 1 + i\sqrt{3},\ -2 \text{ und } 1 - i\sqrt{3}.$$

Um nun einen genaueren Einblick in die entwickelte Theorie zu thun, soll dieselbe auf eine geometrische Untersuchung angewendet werden.

Wie bekannt wird der Ausdruck

$$\frac{x_2 - x_1}{x_3 - x_2} : \frac{x_1 - x_4}{x_4 - x_3}$$

nicht verändert, wenn man die Grössen x_1, x_2, x_3 und x_4 mit ihren reciproken Werthen vertauscht. Diese Grössen sollen complex sein und in der Ebene die Punkte A_1, A_2,

A_3 und A_4 darstellen; dann würde $x_2 - x_1$ die Strecke $A_1 A_2$ ihrer Grösse und Richtung nach bestimmen. Durchläuft man die 4 Strecken in der Reihenfolge $A_1 A_2 A_3 A_4$, bezeichnet die Moduln oder die Seitenlängen mit r_1, r_2, r_3, r_4, und durch die entsprechenden grossen Buchstaben ihre positiven Richtungen, dann wird

$$x_2 - x_1 = r_{1(XR_1)} \text{ u. s. w.,}$$

wo X die positive Richtung bezeichnet.

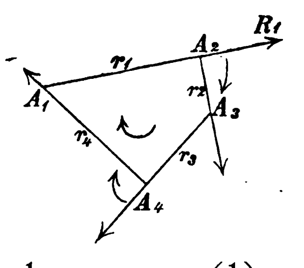
Der gegebene Quotient wäre dann

$$\frac{r_{1(XR_1)}}{r_{2(XR_2)}} : \frac{r_{4(XR_4)}}{r_{3(XR_3)}},$$

dessen Modulus $\frac{r_1 r_3}{r_2 r_4}$ und dessen Argument

$$(XR_1) + (R_2X) + (R_4X) + (XR_3) = (R_2R_1) + (R_4R_3).$$

Der Modulus des Ausdrucks ist also das Verhältniss zwischen den Producten der gegenüberliegenden Seiten, sein Argument die Summe zweier gegenüber liegender Winkel (der Nebenwinkel der Polygonwinkel). Diese Grössen müssen also nach der Vertauschung



dieselben bleiben. Nun wird x mit $\frac{1}{x}$ oder r_θ mit $\left(\frac{1}{r}\right)_{-\theta}$ vertauscht. Verändert man $-\theta$ in θ, so wird dieser Punkt nur mit dem vertauscht, welcher symmetrisch zu demselben mit Beziehung auf die Axe liegt, wobei indessen zugleich die positive Umlaufsrichtung verändert wird. Man gelangt dadurch zu dem Punkte $\left(\frac{1}{r}\right)_\theta$. Der Satz gilt also, wenn jeder Punkt mit einem andern vertauscht wird, welcher auf der Verbindungslinie des Anfangspunktes mit dem gegebenen Punkte so liegt, dass das Product der Abstände der beiden Punkte vom Anfangspunkte gleich 1 ist. Eine solche Ver-

tauschung von Punkten nennt man *Transformation durch reciproke Radien.* Durch einfache Deutung eines algebraischen Satzes ist also bewiesen, dass durch eine solche Transformation bei einem beliebigen Viereck das Verhältniss zwischen den Producten der gegenüberliegenden Seiten und die Summe der gegenüberliegenden Winkel unverändert bleibt. Es thut nichts zur Sache, ob das Viereck ein sogenanntes uneigentliches Viereck ist, wenn nur der Begriff »gegenüberliegende Winkel« auf die aus der voranstehenden Entwicklung folgende Weise gefasst wird.

Ganze rationale Functionen.

4. *In der ganzen rationalen Function*

$$f(z) = A_0 z^m + A_1 z^{m-1} + \ldots . A_{m-1} z \ldots . (1)$$

kann dem mod. z immer ein so kleiner Werth r gegeben werden, dass mod. f(z) für diesen und kleinere Werthe von mod. z kleiner wird als irgend welche gegebene Grösse R.

Wird der grösste Modulus der Coefficienten a genannt, so hat man nämlich

$$\text{mod.}\, f(z) < a(r^m + r^{m-1} \ldots + r) = a \frac{r - r^{m+1}}{1 - r}$$

oder, wenn $r < 1$,

$$\text{mod.}\, f(z) < \frac{a\,r}{1 - r};$$

diese Grösse wird kleiner als R, wenn

$$r < \frac{R}{a + R}$$

genommen wird.

Hieraus folgt zugleich, dass man in der Function

$$z^n + P,$$

wo P eine Function bedeutet, deren Exponenten sämmtlich grösser sind als n, den mod. z so klein machen kann, dass

mod. $\frac{P}{z^n}$ kleiner wird als irgend welche gegebene Grösse; vertauscht man z gegen $\frac{1}{z}$, so sieht man ferner, dass man in

$$z^n + P,$$

wo alle Exponenten in P kleiner sind als n, den mod. z so gross machen kann, dass

$$\text{mod.} \frac{z^n}{P}$$

grösser wird als eine beliebige gegebene Grösse.

5. *Eine ganze rationale Function ist continuirlich.*

$f(z)$ heisst continuirlich, wenn mod. h so klein genommen werden kann, dass der Modulus von

$$f(z+h) - f(z)$$

für alle Werthe von z kleiner wird als irgend eine gegebene, noch so kleine Grösse. Nun nimmt diese Differenz unter Anwendung der Taylorschen Formel die Form

$$f'(z)\,h + f''(z)\frac{h^2}{1 \cdot 2} \cdots + f^{(m)}(z)\frac{h^m}{m!}$$

an, und diese kann, wie eben gezeigt, so klein werden, wie man will, wenn man mod. h hinreichend klein wählt.

Sind die Coefficienten reell, und liefert die Function für 2 reelle Werthe von z Werthe mit entgegengesetztem Vorzeichen, so muss sie gleich Null werden für einen Werth von z, der zwischen den beiden gegebenen liegt.

6. *Eine ganze reelle Function von zwei reellen Variablen x und y kann nicht, wenn x und y sich continuirlich verändern, das Vorzeichen wechseln ohne durch 0 hindurchzugehen.*

Im entgegengesetzten Falle müsste nämlich die Function an einem gewissen Punkte einen Sprung vom Positiven zum Negativen oder umgekehrt machen, so dass $f(x+h, y+k) - f(x, y)$ nicht unter einen gewissen Werth herabgebracht werden könnte, wie klein man auch h und k nehmen möge.

Das ist indessen unmöglich; denn schreibt man die Differenz folgendermassen:

$$f(x+h, y+k) - f(x+h, y) + f(x+h, y) - f(x, y),$$

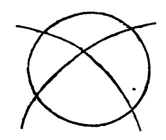
so folgt aus dem vorhergehenden, dass jede der beiden Differenzen, die eine für ein hinreichend kleines k, die andere für ein hinreichend kleines h, kleiner werden kann, als irgend welche gegebene Grösse.

Die algebraische Curve, deren Gleichung $f(x, y) = 0$ ist, theilt die Ebene in verschiedene endliche oder unendliche Theile; betrachtet man zwei Punkte, deren Coordinaten, in $f(x, y)$ eingesetzt, Resultate mit entgegengesetzten Vorzeichen geben, so müssen diese also so liegen, dass man mittelst einer continuirlichen Bewegung nicht von dem einen zum andern gelangen kann ohne die Curve zu passiren; die Theile der Ebene sollen positiv oder negativ mit Bezug auf diese Curve heissen, je nachdem die Punkte beim Einsetzen in die Gleichung ein positives oder negatives Resultat geben; um von einem positiven zu einem negativen Theile zu kommen, muss man die Curve eine ungerade Anzahl Male passiren, um von einem positiven zu einem positiven zu gelangen eine gerade Anzahl Male. Geht man durch einen Punkt der Curve, welcher zweien Curvenästen gemeinsam ist, so muss das als ein zweimaliges Passiren der Curve aufgefasst werden.

Da man $f(x, y)$ mit einem beliebigen Vorzeichen schreiben kann, so ist das Vorzeichen für einen bestimmten Theil willkürlich; kommt man aber überein $f(x, y)$ so zu schreiben, dass das Glied, welches x oder y nicht enthält, positiv ist, so wird der Theil positiv, in welchem der Anfangspunkt liegt, und damit ist dann das Vorzeichen für alle übrigen Theile bestimmt.

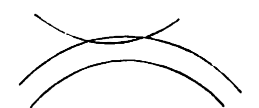
7. Betrachtet man zwei solche Curven, $A = 0$ und $B = 0$, so theilen sie die Ebene in verschiedene Theile, für welche das Product AB positiv oder negativ wird, jenachdem dieselben mit Bezug auf A und B gleiche oder verschiedene Vorzeichen haben. Wählt man irgend einen Durchschnittspunkt der beiden Curven und zeichnet darum eine kleine geschlossene Curve, so wird diese von den Curvenästen in

vier Theile getheilt; durchläuft man die kleine Curve indem man die Werthe von AB für alle ihre Punkte bestimmt, so



bemerkt man, dass AB jedesmal gleich Null wird und das Vorzeichen wechselt, wenn ein Curvenast passirt wird. Nennt man die Stücke der kleinen Curve positiv oder negativ, je nachdem die Punkte dieser Stücke AB positiv oder negativ machen, so werden zwei gegenüberliegende Stücke positiv, die beiden anderen negativ. Bei dem Passiren der einen Curve erfolgt jedesmal ein Uebergang vom Positiven zum Negativen, bei dem Passiren der anderen vom Negativen zum Positiven. Wird eine bestimmte Umlaufsrichtung innegehalten, so sieht man, dass sich zwei Arten von Durchschnittspunkten ergeben, nämlich solche, wo beim Passiren der Curve A ein Uebergang vom Positiven zum Negativen erfolgt, und solche, wo beim Passiren von A ein Uebergang vom Negativen zum Positiven stattfindet. Beispielsweise findet man, dass die Durchschnittspunkte zweier Kreise jeder von besonderer Art sind.

Bildet man für jeden Durchschnittspunkt der Curven A und B den Unterschied zwischen der Anzahl Male, wo man beim Umlauf in positiver Richtung und beim Passiren von A den Uebergang vom Positiven zum Negativen macht, und der Anzahl Male, wo man den Uebergang vom Negativen zum Positiven macht, so erhält man die Zahl $+2$ bei allen Durchschnittspunkten der einen Art, und -2 bei allen Durchschnittspunkten der anderen Art. Durch Addition aller dieser Differenzen erhält man also eine Zahl, welche doppelt so gross ist, wie der Unterschied zwischen der Anzahl der Durchschnittspunkte der ersten Art und der Anzahl der Durchschnittspunkte der zweiten Art. Diese Zahl muss übrigens dieselbe sein, welche man bekommt, wenn man auf dieselbe Weise den Umfang einer beliebigen geschlossenen Curve durchläuft, welche alle Durchschnittspunkte umschliesst. Wenn sich nämlich eine solche Curve verändert, kann sich die Reihenfolge, in welcher ihre Durchschnittspunkte mit A und B vorkommen, jedesmal nur dann ändern, wenn man



einen Durchschnittspunkt von A und B passirt, und wenn die Curve, indem sie eine Stellung verlässt, in welcher sie A oder B berührt, zwei Durchschnittspunkte mit einer dieser Curven bekommt oder verliert. Diese letzteren Durchschnittspunkte können indessen keinen Einfluss auf die gesuchte Differenz haben, da sie unmittelbar auf einander folgen; sind es Durchschnittspunkte mit B, so werden sie nicht mitgerechnet, und sind es Durchschnittspunkte mit A, so verändern sie die Differenz nicht, weil bei dem einen der Uebergang vom Positiven zum Negativen, bei dem andern der Uebergang vom Negativen zum Positiven erfolgen muss. Da nun zugleich 2 solche Punkte, weil sie zusammen auftreten, keinen Einfluss auf die Vorzeichen bei den übrigen Durchschnittspunkten haben können, so sieht man, dass sie überhaupt keinen Einfluss auf die gesuchte Differenz haben. Diese kann sich also nur dann ändern, wenn man die Curve sich so verändern lässt, dass sie einen der Durchschnittspunkte von A und B passirt.

Man nehme eine kleine geschlossene Curve an, welche weder A noch B schneidet, und für welche die Differenz also gleich Null ist. Darauf lasse man dieselbe sich erweitern, und jedesmal wenn sie dadurch eine der kleinen Curven berührt, welche um einen Durchschnittspunkt beschrieben sind, lasse man sie diese und dadurch den Durchschnittspunkt umschliessen; die Differenz wird dadurch um + 2 oder — 2 vermehrt, je nachdem der Durchschnittspunkt von der ersten oder der zweiten Art ist; dergestalt ist folgender Satz bewiesen:

Sind zwei Curven A und B gegeben, und durchläuft man eine beliebige geschlossene Curve in einer bestimmten Umlaufsrichtung, so wird die Zahl, welche den Unterschied zwischen der Anzahl der beiden Arten von Durchschnittspunkten innerhalb der geschlossenen Curve angiebt, halb so gross sein wie der Unterschied zwischen der Anzahl Male, wo beim Passiren

von A ein Uebergang vom Positiven zum Negativen, und der Anzahl Male, wo ein Zeichenwechsel im entgegengesetzten Sinne stattfindet.

Giebt es nur Durchschnittspunkte der einen Art, so bestimmt man auf diese Weise, wie viele reelle Durchschnittspunkte die Curven innerhalb der geschlossenen Curve haben. Der Satz gilt immer, wie nahe auch die Durchschnittspunkte beisammen liegen; fallen mehrere zusammen, so gilt er also, wenn man statt dieses einen Punktes so viele zählt, wie hier zusammengefallen sind.

Anzahl der Wurzeln einer Gleichung.

8. Es sei die Gleichung n^{ten} Grades

$$f(z) = A_0 z^n + A_1 z^{n-1} + \dots A_n = 0 \quad \dots\dots\dots (1)$$

gegeben, worin die Coefficienten reell oder imaginär sein können. Setzt man

$$z = x + yi,$$

wo x und y reell sind, so erhält man durch Trennung der reellen und imaginären Glieder

$$f(x + yi) = A + Bi, \quad \dots\dots\dots (2)$$

worin A und B gewisse reelle Functionen von x und y sind. Die nothwendigen und ausreichenden Bedingungen dafür, dass $x + yi$ eine Wurzel der Gleichung (1) sei, sind

$$A = 0; \; B = 0. \quad \dots\dots\dots (3)$$

Die Wurzeln werden also durch die reellen Durchschnittspunkte der beiden Curven A und B repräsentirt, die sogenannten *Wurzelpunkte.**)

---

*) Die Curven A und B können nicht beliebig sein, sondern müssen immer auf eine gewisse Weise von einander abhängen. Man erhält nämlich durch partielle Differentiation der Identität (2)

$$f'(x + yi) = \frac{dA}{dx} + \frac{dB}{dx} i;$$

$$i f'(x + yi) = \frac{dA}{dy} + \frac{dB}{dy} i,$$

woraus folgt

$$\frac{dB}{dx} = -\frac{dA}{dy}; \; \frac{dA}{dx} = \frac{dB}{dy}.$$

Nun soll der eben gefundene Satz auf diese Curven angewendet werden, und man denke sich deshalb einen Kreis, der so gross ist, dass er alle Durchschnittspunkte, falls es solche giebt, umschliesst; dividirt man die Gleichung (1) durch A_0, so erhält man die Form

$$z^n + a_\upsilon z^{n-1} + \ldots\ldots = 0, \quad \ldots\ldots\ldots\ldots \quad (4)$$

und hieraus, indem $z = x + yi = r(\cos\theta + i\sin\theta)$,

$$A = r^n \cos n\theta + a r^{n-1} \cos[(n-1)\theta + \upsilon] + \ldots = 0 \quad \ldots\ldots \quad (5)$$

$$B = r^n \sin n\theta + a r^{n-1} \sin[(n-1)\theta + \upsilon] + \ldots = 0 \quad \ldots\ldots \quad (6)$$

Man kann den Kreis, also r, so gross machen, dass dessen Durchschnittspunkte mit A und B mit so grosser Annäherung, wie man will, durch das erste Glied bestimmt werden; das giebt beziehungsweise für A uud B

$$\cos n\theta = 0; \ \sin n\theta = 0,$$

woraus

$$\theta = \frac{(2p+1)\pi}{2n}; \ \theta = \frac{p\pi}{n}.$$

Hieraus sieht man, dass die Durchschnittspunkte mit den beiden Curven, je grösser der Kreis wird, um so mehr sich den Stellungen nähern, in welchen sie die Peripherie in 4n gleich grosse Theile theilen, und dass die Durchschnittspunkte mit A und B abwechselnd auf einander folgen. Da die früher besprochene Differenz solchergestalt 2n wird, muss der Unterschied zwischen den Anzahlen der beiden Arten von Durchschnittspunkten n sein, und es müssen also wenigstens n der einen Art vorhanden sein.

Eine Gleichung n^{ten} Grades hat also wenigstens n Wurzeln.

9. *Ist α_1 eine Wurzel der Gleichung $f(z) = 0$, so ist das Polynom $f(z)$ theilbar durch $z - \alpha_1$.*

Man kann nämlich in jedem Fall

$$f(z) = (z - \alpha_1)\,Q + R$$

setzen, worin Q eine ganze Function bedeutet, und R z

nicht enthält. Diese Identität muss auch gelten für $z = \alpha_1$, und dadurch erhält man

$$R = 0,$$

da z nicht in R enthalten ist, und R also unverändert bleibt, wenn man α_1 für z einsetzt.

Ist α_2 eine andere Wurzel der Gleichung, so muss durch dieselbe $(z - \alpha_1) Q$, also auch Q gleich Null werden. Folglich ist

$$Q = (z - \alpha_2) Q_1,$$

also

$$f(z) = (z - \alpha_1)(z - \alpha_2) Q_1$$

und so fort.

Umgekehrt sieht man leicht, *dass* α *eine Wurzel von* $f(z) = 0$ *ist, wenn* $z - \alpha$ *ein Factor von* $f(z)$ *ist.* Jeder Wurzel von $f(z) = 0$ entspricht also ein Factor von $f(z)$ von der Form $z - \alpha$ und umgekehrt. Da nun ein Polynom des n^{ten} Grades nicht mehr als n Factoren ersten Grades enthalten kann, so kann eine Gleichung n^{ten} Grades nicht mehr als n Wurzeln haben. In Verbindung mit dem Satze in 8 geht hieraus hervor, dass *eine Gleichung* n^{ten} *Grades immer n Wurzeln hat.**) Sind diese $\alpha_1, \alpha_2 \ldots \alpha_n$, so ist

$$f(z) = A_0 (z - \alpha_1)(z - \alpha_2) \ldots (z - \alpha_n), \quad \ldots\ldots\ldots (7)$$

wo A_0 der Coefficient von z^n in $f(z)$ ist.

---

*) Hieraus folgt wieder, dass alle Wurzelpunkte von derselben Art sein müssen, so dass man den oben gefundenen Satz anwenden kann um die Anzahl der Wurzelpunkte innerhalb einer beliebigen geschlossenen Curve zu bestimmen (Satz von Cauchy).

Man kann beweisen, dass die beiden Arten von Durchschnittspunkten für zwei beliebige Curven A und B so liegen, dass man die Curve

$$\frac{dA}{dx}\frac{dB}{dy} - \frac{dA}{dy}\frac{dB}{dx} = 0$$

eine ungerade Anzahl Male passiren muss, um von einem Durchschnittspunkte der einen Art zu einem der andern Art zu gelangen. Diese Curve erhält keine reellen Aeste, wenn $A = 0$ und $B = 0$ die Wurzelpunktcurven sind. (Cfr. Anm. S. 15.)

10. Der geführte Beweis setzte voraus, dass alle Durchschnittspunkte von A und B einfache Durchschnittspunkte waren, d. h. solche, wo man auf der kleinen geschlossenen Curve A und B abwechselnd traf und jede zwei Male. Ist dies nicht der Fall, so erhält man die n Wurzeln nur dadurch, dass man einen solchen Durchschnittspunkt von besonderer Natur so oft mitzählt, wie eine kleine um denselben beschriebene geschlossene Curve durch die Uebergänge von + zu — angiebt; dieser Fall soll nun genauer untersucht werden.

Wird ein Wurzelpunkt, der $z = \alpha$ entspricht, zum Anfangspunkt genommen, so muss $z = 0$ der Gleichung genügen und diese also die Form

$$a_{\upsilon} z + b_{\upsilon_1} z^2 \ldots = 0 \ldots \ldots \ldots \ldots \quad (8)$$

annehmen, woraus

$$A = a r \cos(\theta + \upsilon) + b r^2 \cos(2\theta + \upsilon_1) + \ldots = 0; \ldots \quad (9)$$

$$B = a r \sin(\theta + \upsilon) + b r^2 \sin(2\theta + \upsilon_1) + \ldots = 0, \ldots \quad (10)$$

und hierin braucht man, für ein hinreichend kleines r, nur das erste Glied zu berücksichtigen. Solange a also nicht gleich Null ist, erhält jede Curve nur zwei Durchschnittspunkte mit einem kleinen Kreise mit dem Radius r, nämlich die, welche durch $\cos(\theta + \upsilon) = 0$ für A, und $\sin(\theta + \upsilon) = 0$ für B bestimmt werden. Man hat es also mit einem gewöhnlichen Durchschnittspunkte zu thun; ist dagegen $a = 0$, so werden die Durchschnittspunkte beziehungsweise durch

$$\cos(2\theta + \upsilon_1) = 0 \text{ und } \sin(2\theta + \upsilon_1) = 0$$

bestimmt, woraus hervorgeht, dass jede der Curven in diesem Punkte einen Doppelpunkt besitzt, so dass der Kreis die beiden Curven in 8 Punkten schneidet, da jede der Gleichungen 4 Werthe für θ giebt; da diese nun abwechseln, so wird ein solcher Punkt die Differenz um ± 4 vermehren und also wie 2 Wurzelpunkte zählen. Im Allgemeinen findet man, dass der Punkt wie p Wurzelpunkte gezählt werden muss, wenn die Gleichung mit z^p anfängt, oder wenn ihre linke Seite durch z^p theilbar ist. In diesem Falle ist f(z) theilbar

durch $(z - \alpha)^p$, und man sieht dergestalt, dass *der aufgestellte Satz über die Anzahl der Wurzeln nur gilt, wenn eine Wurzel* α *wie p Wurzeln gezählt wird, sobald* $f(z)$ *theilbar ist durch* $(z - \alpha)^p$. Man sagt, dass die Gleichung in diesem Falle *gleiche Wurzeln* habe und nennt α eine p fache Wurzel.

11. *Zweiter Beweis dafür, dass eine Gleichung* n^{ten} *Grades n Wurzeln hat* (Beweis von Argand, auch Cauchy's Beweis genannt).

Es genügt, wenn man nachweisen kann, dass jede Gleichung wenigstens eine Wurzel hat, denn man kann sich dann den dieser Wurzel entsprechenden Factor durch Division entfernt denken; dadurch gelangt man zu einer Gleichung, welche um einen Grad niedriger ist und welche wiederum eine Wurzel haben muss; durch Fortsetzung dieses Verfahrens erhält man schliesslich eine Gleichung ersten Grades, welche eine Wurzel hat, und man hat dann nach und nach n Wurzeln bestimmt, falls die Gleichung vom n^{ten} Grade war.

Um nun zu zeigen, dass

$$f(z) = 0$$

wenigstens eine Wurzel hat, untersuchen wir, ob ein gewisser Werth

$$z_0 = r_\theta$$

der Gleichung Genüge leistet; thut er das, so hat man eine Wurzel; thut er es nicht, so erhält $f(z)$ dadurch einen gewissen Werth Z_0 mit dem Modulus R, aber man kann dann zeigen, dass man durch kleine an r und θ vorgenommene Veränderungen einen anderen Werth von $f(z)$ mit einem kleineren Modulus als R erhalten kann, so lange R nicht Null ist. Setzt man nämlich $z_0 + h$ an die Stelle von z_0, worin

$$h = \rho_\omega,$$

so erhält man

$$f(z_0 + h) = f(z_0) + f^p(z_0)\frac{h^p}{p!} + f^{p+1}(z_0)\frac{h^{p+1}}{(p+1)!} + \dots A_0 h^n,$$

wo $p \gtreqless 1$ sein kann, da einige der abgeleiteten Functionen Null werden können. Man erhält dann

$$\frac{f(z_0 + h)}{f(z_0)} = 1 + C_p \rho^p \left[\cos(p\omega + \alpha_p) + i \sin(p\omega + \alpha_p)\right] + B,$$

worin B theilbar ist durch eine höhere Potenz von ρ als ρ^p und worin

$$\frac{f^p(z_0)}{p! f(z_0)} = C_p (\cos \alpha_p + i \sin \alpha_p),$$

so dass C_p eine positive Grösse ist, welche nicht Null sein kann.

Wählt man nun ω so, dass

$$p\omega + \alpha_p = \pi,$$

so erhält man

$$\cos(p\omega + \alpha_p) = -1; \sin(p\omega + \alpha_p) = 0.$$

also

$$\frac{f(z_0 + h)}{f(z_0)} = 1 - C_p \rho^p + B_0,$$

worin B_0 der Werth von B ist, welcher dem eingesetzten Werthe von ω entspricht. Das Glied $-C_p \rho^p$ ist negativ und für hinreichend kleine Werthe von ρ grösser als mod. B_0; man kann also immer ω und ρ so wählen, dass

$$\text{mod.} \frac{f(z_0 + h)}{f(z_0)} < 1 \text{ oder mod.} f(z_0 + h) < \text{mod.} f(z_0).$$

Es kann deshalb keine möglichst kleinen Werthe von R geben ausser Null, und dadurch ist der Satz bewiesen.

Man könnte sich doch die Möglichkeit denken, dass man bei einem beständig abnehmenden R sich einer gewissen Grenze, welche von Null verschieden wäre, näherte ohne sie zu erreichen; denkt man sich indessen alle Werthe von R, welche allen möglichen endlichen Werthen von z entsprechen, so muss einer von ihnen der kleinste sein, aber das ist, wie gezeigt worden, unmöglich für andere Werthe als Null. Es bleibt dann nur noch die Möglichkeit, dass z

bis ins Unendliche wächst, wenn R abnimmt, aber das kann nicht der Fall sein, da f(z) zugleich mit z ohne Grenze wächst.

Conjugirte Wurzeln in Gleichungen mit reellen Coefficienten.

12. *Ist die complexe Grösse $a + bi$ eine Wurzel einer Gleichung mit reellen Coefficienten, so ist $a - bi$ auch eine Wurzel der Gleichung.*

In diesem Fall hat man nämlich

$$f(z) = [z - (a + bi)]\, Q,$$

wo Q ein ganzes Polynom bedeutet. Da i in f(z) nicht vorkommt, muss i wegfallen, wenn die Multiplication auf der rechten Seite ausgeführt wird; das kann indessen nur dadurch geschehen, dass i überall gerade Exponenten bekommt, und wenn das der Fall ist, so wird der Ausdruck nicht verändert werden, wenn man $+i$ mit $-i$ vertauscht. Dadurch erhält man

$$f(z) = [z - (a - bi)]\, Q_1,$$

wo Q_1 die ganze Function bedeutet, welche aus Q durch die Vertauschung von $+i$ mit $-i$ gebildet wird. Man sieht also, dass f(z) auch theilbar ist durch $z - (a - bi)$, oder dass $a - bi$ auch eine Wurzel der Gleichung ist.

Die complexen Wurzeln in einer solchen Gleichung kommen also paarweise vor, und dasselbe muss dann auch für die complexen Factoren in f(z) gelten.

Durch Zusammenziehen zweier solcher Factoren erhält man den reellen Factor

$$(z - a)^2 + b^2;$$

man sieht hieraus, dass man sich ein reelles Polynom stets in lauter reelle Factoren aufgelöst denken kann, welche theils vom ersten und theils vom zweiten Grade sind.

Bestimmung der zwei Gleichungen gemeinschaftlichen Wurzeln.

13. Falls die beiden Gleichungen

$$f(z) = 0 \text{ und } F(z) = 0$$

die Wurzeln a, b, c... gemeinschaftlich haben, müssen f(z) und F(z) den gemeinschaftlichen Factor $(z-a)(z-b)(z-c)\ldots$ haben und umgekehrt. Da man nun durch bekannte Mittel immer den grössten gemeinschaftlichen Factor zweier Polynome bestimmen kann, so kann man dadurch immer die Gleichung finden, welche die für zwei gegebene Gleichungen gemeinschaftlichen Wurzeln bestimmt. Solche Gleichungen werden dadurch auf einen niedrigeren Grad reducirt. Ist z. B. $\varphi(z)$ der grösste gemeinschaftliche Factor für f(z) und F(z), so erhält man durch Auflösung der Gleichung $\varphi(z) = 0$ alle gemeinschaftlichen Wurzeln. Die übrigen Wurzeln der beiden Gleichungen werden dann durch die Gleichungen

$$\frac{f(z)}{\varphi(z)} = 0 \text{ und } \frac{F(z)}{\varphi(z)} = 0 \text{ . . . . } (2)$$

bestimmt.

Für den Fall, dass die gemeinschaftlichen Wurzeln in den gegebenen Gleichungen als gleiche Wurzeln vorkommen, wird $\varphi(z) = 0$ die Wurzeln in der kleinsten Anzahl Male, in der sie vorkommen, enthalten. Ist z. B. f(z) theilbar durch $(z-\alpha)^p$ und F(z) theilbar durch $(z-\alpha)^{p+q}$, so wird, wie bekannt, $\varphi(z)$ theilbar werden durch $(z-\alpha)^p$; man kann dann die Aufgabe noch weiter reduciren, da die zweite Gleichung (2) und $\varphi(z) = 0$ wieder gemeinschaftliche Wurzeln bekommen, und also auf dieselbe Weise behandelt werden können.

Falls $f(z)$ in rationale Factoren zerlegt werden kann, soll die Gleichung $f(z) = 0$ reductibel heissen, im entgegengesetzten Fall *irreductibel.*

Da nun $\varphi(z)$ rational wird, wenn f(z) und F(z) es sind, so sieht man, dass zwei Gleichungen reductibel sein müssen, wenn sie gemeinschaftliche Wurzeln haben; doch ist es

möglich, dass z. B. $f(z)$ in $F(z)$ aufgeht, so dass $\varphi(z) = f(z)$. In diesem Fall kann $f(z) = 0$ irreductibel sein.

Hieraus folgt also, *dass eine Gleichung, welche eine Wurzel mit einer irreductiblen Gleichung gemein hat, alle Wurzeln derselben haben muss.*

Bedingungen dafür, dass zwei Gleichungen gemeinschaftliche Wurzeln haben.

14. Es lässt sich die Bedingung angeben, welche die Coefficienten zweier Gleichungen erfüllen müssen, damit die Gleichungen eine Wurzel gemeinschaftlich haben. Es seien die Gleichungen

$$f(z) = z^n + a_1 z^{n-1} + a_2 z^{n-2} \ldots + a_n = 0 \quad \ldots\ldots \quad (1)$$

und

$$f_1(z) = z^m + b_1 z^{m-1} + b_2 z^{m-2} \ldots + b_m = 0. \quad \ldots\ldots \quad (2)$$

Falls die Gleichungen eine Wurzel gemeinschaftlich haben, müssen $f(z)$ und $f_1(z)$ einen gemeinschaftlichen Factor vom ersten Grade haben; sucht man den grössten gemeinschaftlichen Factor von $f(z)$ und $f_1(z)$, so erhält man zuletzt einen Rest, der nur Coefficienten der Gleichungen enthält; nachdem durch Division aus diesem die Factoren entfernt sind, welche während des Verlaufs der Rechnung eingeführt wurden um Brüche zu vermeiden, sei derselbe V; dann würde

$$V = 0 \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (3)$$

die nothwendige und ausreichende Bedingung dafür sein, dass die beiden Polynome einen gemeinschaftlichen Factor vom ersten Grade haben, oder dass die beiden Gleichungen eine gemeinschaftliche Wurzel besitzen. Der nächstletzte Rest hat die Form

$$V_1 z + V_2.$$

Ist dieser gleich Null, so haben die Polynome einen gemeinschaftlichen Factor vom 2ten Grade und die Gleichungen

besitzen also zwei gemeinschaftliche Wurzeln; die Bedingungen für zwei gemeinschaftliche Wurzeln sind also

$$V_1 = 0;\ V_2 = 0 \ldots\ldots\ldots\ldots\ldots \quad (4)$$

und so fort.

15. Lagrange hat den Bedingungsgleichungen eine andere Form gegeben, wodurch ihre Bedeutung allerdings auch etwas abweichend von der der obenstehenden Gleichungen wird. Man denke sich einen der Coefficienten a in der einen Gleichung veränderlich, während im Uebrigen die Coefficienten beider Gleichungen unverändert bleiben. Indem a sich continuirlich verändert, ändern sich zugleich die Wurzeln der Gleichung, und für gewisse Werthe von a passiren sie die Wurzeln der andern Gleichung; man kan den Zuwachs h suchen, welchen man zu a hinzufügen muss, damit die neue Gleichung (1) eine Wurzel mit der unveränderten Gleichung (2) gemeinsam habe.

Wird in V für a der Werth a + h eingesetzt, so erhält man einen neuen Werth V_1, der bestimmt wird durch

$$V_1 = V + \frac{dV}{da} h + \frac{d^2 V}{da^2} \frac{h^2}{1.2} + \ldots\ldots\ldots\ldots \quad (5)$$

Ist der Werth von a, von welchem ausgegegangen wurde, so beschaffen, dass es für ihn eine gemeinschaftliche Wurzel giebt, so ist V = 0, und soll man für den Werth a + h auch eine gemeinschaftliche Wurzel haben, so muss $V_1 = 0$ sein. Der Zuwachs h wird deshalb bestimmt durch die Gleichung

$$\frac{dV}{da} h + \frac{d^2 V}{da^2} \frac{h^2}{1.2} + \frac{d^3 V}{da^3} \frac{h^3}{1.2.3} + \ldots = 0 \ldots\ldots \quad (6)$$

Denkt man sich alle Wurzeln von (2) in (1) eingesetzt, so erhält man für jede derselben den Werth von a bestimmt, welcher (1) genügt, und jedem von diesen entspricht ein Werth von h in (6). Die m verschiedenen Werthe von h entsprechen deshalb einzeln ihrer Wurzel von (2). Auf der anderen Seite können zwei Gleichungen (1), welche verschiedenen Werthen von a entsprechen, keine gemeinschaftliche Wurzel haben (ausgenommen x = 0, wovon man absehen kann). Soll

nun für einen Werth von a der Gleichung (1) Genüge geleistet werden durch q Wurzeln der Gleichung (2), so muss (6) q Wurzeln erhalten, welche Null sind; *die nothwendigen und ausreichenden Bedingungen dafür, dass q Wurzeln von (2) der Gleichung (1) genügen, sind deshalb:*

$$V = 0;\ \frac{dV}{da} = 0;\ \frac{d^2V}{da^2} = 0\ldots;\ \frac{d^{q-1}V}{da^{q-1}} = 0, \ldots\ldots \quad (7)$$

wobei nur vorausgesetzt ist, dass $x = 0$ keine Wurzel ist.

Diese Gleichungen drücken dasselbe aus, wie die früher gefundenen, wenn die q Wurzeln verschieden sind; kommt dagegen z. B. die Wurzel α mehrere Male unter denselben vor, braucht sie doch nur einmal in (1) vorzukommen, wenn den Gleichungen (7) Genüge geleistet ist. Man sieht leicht, dass man statt eines der Coefficienten eine Grösse nehmen kann, von welcher mehrere der Coefficienten lineare Functionen sind; ist diese p, wird die Gleichung also die Form

$$A + pB = 0$$

haben, und eine der obigen analoge Untersuchung wird zeigen, dass man annehmen muss, A und B haben keinen gemeinschaftlichen Factor.

Gleiche Wurzeln.

16. *Jede Grösse, welche ein oder mehrere Male Wurzel von $f(z) = 0$ ist, ist ein Mal weniger Wurzel von $f'(z) = 0$.*

Sei z. B. α p Male Wurzel von $f(z) = 0$; dann ist

$$f(z) = (z - a)^p Q,$$

wo q nicht theilbar ist durch $z - \alpha$. Hieraus erhält man

$$\begin{aligned} f'(z) &= p(z-\alpha)^{p-1} Q + (z-\alpha)^p Q' \\ &= (z-\alpha)^{p-1} [pQ + (z-a) Q'], \end{aligned}$$

wo Q' die abgeleitete Function von Q bedeutet. $f'(z)$ ist also theilbar durch $(z - \alpha)^{p-1}$ und durch keine höhere Potenz

von $z - \alpha$, da $z - \alpha$ nicht in pQ aufgeht. α kommt also $p - 1$ Male als Wurzel in $f'(z) = 0$ vor.

Bezeichnet nun P_1 das Product der Factoren von $f(z)$, welche jeder nur ein Mal vorkommen, P_2 das Product der Factoren, welche jeder zwei Male vorkommen u. s. w., so ist

$$f(z) = P_1 P_2^2 P_3^3 \ldots$$

$$f'(z) = P_2 P_3^2 \ldots Q,$$

wo Q die Factoren von $f'(z)$ enthält, welche für die gleichen Wurzeln nicht in Betracht kommen. Für den grössten gemeinschaftlichen Factor von $f(z)$ und $f'(z)$ erhält man nun

$$\varphi(z) = P_2 P_3^2 \ldots,$$

woraus

$$\frac{f(z)}{\varphi(z)} = P_1 P_2 P_3 \ldots = f_1(z).$$

Sucht man nun den grössten gemeinschaftlichen Factor $\varphi_1(z)$ für $\varphi(z)$ und deren Abgeleitete, so erhält man, wenn man $\varphi(z)$ durch $\varphi_1(z)$ dividirt

$$f_2(z) = P_2 P_3 \ldots$$

und daraus

$$\frac{f_1(z)}{f_2(z)} = P_1.$$

Dergestalt ist die Gleichung

$$P_1 = 0$$

gefunden, und diese bestimmt alle die Wurzeln, welche nur einmal in der gegebenen Gleichung vorkommen. Diese Gleichung ist im Allgemeinen irreductibel, und es wird deshalb von ihrem Grade abhängen, ob sie auflösbar ist oder nicht.

Zur Bestimmung von P_2 hat man

$$\varphi_1(z) = P_3 P_4^2 \ldots,$$

folglich, wenn $\varphi_2(z)$ den grössten gemeinschaftlichen Factor für $\varphi_1(z)$ und deren Abgeleitete bedeutet,

$$\frac{\varphi_1(z)}{\varphi_2(z)} = P_3 P_4 \ldots = f_3(z),$$

und daraus wiederum

$$\frac{f_2(z)}{f_3(z)} = P_2.$$

Durch Fortzetzung dieser Methode erhält man nach und nach die Gleichungen

$$P_1 = 0;\ P_2 = 0;\ P_3 = 0 \ldots$$

und durch Auflösung dieser alle Wurzeln von $f(z) = 0$. Diese Gleichungen werden sich, wie schon bemerkt, nicht immer auflösen lassen, aber *man kann jedenfalls immer die Auflösung einer Gleichung mit gleichen Wurzeln zurückführen auf die Auflösung mehrerer Gleichungen ohne gleiche Wurzeln,* und *jede dieser Gleichungen bestimmt ein System von Wurzeln, welche in der gegebenen Gleichung gleich oft vorkommen.*

Die Coefficienten, ausgedrückt durch die Wurzeln.

17. Die allgemeine Form der Gleichung n^{ten} Grades wird, wenn man den Coefficienten von z^n durch Division entfernt,

$$f(z) = z^n + a_1 z^{n-1} + a_2 z^{n-2} \ldots + a_{n-1} z + a_n = 0 \ldots\ldots (1)$$

Sind die Wurzeln $\alpha_1, \alpha_2, \ldots \alpha_n$, so hat man

$$f(z) = (z - \alpha_1)(z - \alpha_2)(z - \alpha_3) \ldots (z - \alpha_n) \ldots\ldots (2)$$

Durch Ausführung dieser Multiplication und durch nachherige Vergleichung der Coefficienten in den beiden Ausdrücken für $f(z)$ erhält man

$$\left.\begin{array}{l} \alpha_1 + \alpha_2 + \ldots \alpha_n = -a_1 \\ \alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \ldots \alpha_{n-1} \alpha_n = a_2 \\ \alpha_1 \alpha_2 \alpha_3 + \alpha_1 \alpha_2 \alpha_4 + \ldots \alpha_{n-2} \alpha_{n-1} \alpha_n = -a_3 \\ \quad\vdots \qquad \vdots \qquad \vdots \qquad \vdots \\ \alpha_1 \alpha_2 \alpha_3 \ldots \alpha_n = (-1)^n a_n. \end{array}\right\} \ldots\ldots (3)$$

Zweites Kapitel.

Beziehungen zwischen Wurzeln und Coefficienten.

Symmetrische Functionen der Wurzeln.

18. Eine Function mehrerer Variablen heisst *symmetrisch,* wenn sie nicht verändert wird durch die Vertauschung von zwei beliebigen der Variablen. Hier sollen nur rationale symmetrische Functionen behandelt werden.

Wenn ein Ausdruck, der keine symmetrische Form hat, an Werth unverändert bleibt bei Vertauschung der ihn zusammensetzenden Grössen, kann derselbe so geschrieben werden, dass auch die Form symmetrisch ist. So bleibt z. B.

$$a^2 + 3b$$

unverändert bei der Vertauschung von a und b, wenn $a = 1$, $b = 2$, aber man kann dann statt dessen schreiben:

$$\frac{1}{2}(a^2 + 3b + b^2 + 3a);$$

allgemein, wenn φ durch Vertauschung die verschiedenen Formen

$$\varphi_1, \varphi_2, \cdots \varphi_n$$

annimmt, die alle denselben Werth haben, so kann man

$$\varphi = \frac{1}{n}(\varphi_1 + \varphi_2 \cdots + \varphi_n)$$

setzen, und dieser Ausdruck ist auch symmetrisch in der Form.

Eine beliebige symmetrische Function der Wurzeln einer Gleichung kann durch die Coefficienten der Gleichung rational ausgedrückt werden.

Falls die Function gebrochen ist, kann sie als Bruch geschrieben werden, und man kann dann Zähler und Nenner desselben einzeln betrachten, da diese auch symmetrische Functionen werden müssen. Wären nämlich Zähler und Nenner des so viel wie möglich verkürzten Bruches

$$\frac{\varphi(x_1, x_2, \ldots)}{\psi(x_1, x_2, \ldots)}$$

keine symmetrischen Functionen, so müsste es zwei Wurzeln geben, welche bei ihrer Vertauschung den Bruch unverändert liessen, während Zähler und Nenner desselben verändert würden. Das ist indessen unmöglich, denn es würde mit sich führen, dass die beiden identischen Brüche nicht für dieselben Werthe von x_1, $x_2 \ldots$ unendlich würden.

Auf die Weise können nur ganze symmetrische Functionen in Betracht kommen. In einer solchen kann man ein Glied wählen, und indem man die darin vorkommenden Wurzeln aus den Wurzeln der Gleichung auf alle möglichen Arten herausnimmt, eine Gruppe von Gliedern erhalten, welche alle in der symmetrischen Function vorkommen müssen, und welche zusammen eine symmetrische Function bilden, die für sich berechnet werden kann; die übrig gebliebenen Glieder werden dann auf dieselbe Weise behandelt. Ist die Gleichung z. B. vom dritten Grade mit den Wurzeln x_1, x_2 und x_3, und kommt in der Function das Glied $x_1 x_2^2 x_3$ vor, so müssen sich auch die Glieder $x_2 x_1^2 x_3$ und $x_1 x_3^2 x_2$ in derselben finden, und man behandelt dann die symmetrische Function

$$x_1 x_2^2 x_3 + x_2 x_1^2 x_3 + x_1 x_3^2 x_2$$

für sich, die wiederum als

$$x_1 x_2 x_3 (x_1 + x_2 + x_3)$$

geschrieben werden kann, so dass man es hier mit den beiden symmetrischen Functionen $x_1 x_2 x_3$ und $x_1 + x_2 + x_3$ zu thun hat.

Eigentlich hätte man hier 6 Glieder erwarten sollen, da die 3 Wurzeln, welche in dem einzelnen Gliede vorkommen, auf 6 Arten permutirt werden können; das einzelne Glied ist inzwischen selber symmetrisch mit Bezug auf die zwei Wurzeln, und deshalb bleiben nur 3 Versetzungen übrig, welche wirklich verschiedene Ausdrücke geben.

Eine symmetrische Function, welche nicht in einfachere symmetrische Functionen zerlegt werden kann, ist also bestimmt durch ein einzelnes von ihren Gliedern; durch ein vor dieses Glied gesetztes Σ soll die durch dasselbe bestimmte symmetrische Function bezeichnet werden; beispielsweise ist also für eine Gleichung n^{ten} Grades:

$$\Sigma x_1 x_2 = x_1 x_2 + x_1 x_3 + x_1 x_4 \ldots + x_{n-1} x_n,$$
$$\Sigma x_1^2 = x_1^2 + x_2^2 \ldots + x_n^2.$$

Newton's Formeln.

19. In Sonderheit sollen die symmetrischen Functionen

$$\Sigma x_1 = s_1;\ \Sigma x_1^2 = s_2 \ldots \Sigma x_1^r = s_r$$

betrachtet werden, zu deren Berechnung Newton folgende Methode angegeben hat:

Aus

$$f(x) = (x - x_1)(x - x_2) \ldots (x - x_n) \quad \ldots\ldots\ldots (1)$$

erhält man, indem man den natürlichen Logarithmus nimmt und differentiirt:

$$\frac{f'(x)}{f(x)} = \frac{1}{x - x_1} + \frac{1}{x - x_2} \ldots + \frac{1}{x - x_n} \text{ *)}, \quad \ldots\ldots (2)$$

---

*) Dieser Satz kann auch auf folgende Weise gefunden werden: Aus

$$f(x) = (x - x_1)(x - x_2) \ldots (x - x_n)$$

erhält man

$$f(x + h) = (x + h - x_1)(x + h - x_2) \ldots (x + h - x_n),$$

also

$$f'(x) = \frac{f(x)}{x-x_1} + \frac{f(x)}{x-x_2} \ldots + \frac{f(x)}{x-x_n} \ldots\ldots\ldots (3)$$

Nun ist aber

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} \ldots + a_n \ldots\ldots\ldots (4)$$

also

$$\frac{f(x)}{x-x_1} = x^{n-1} \begin{array}{l} + x_1 \\ + a_1 \end{array} \left| x^{n-2} \begin{array}{l} + x_1^2 \\ + a_1 x_1 \\ + a_2 \end{array} \right| x^{n-3} \begin{array}{l} + x_1^3 \\ + a_1 x_1^2 \\ + a_2 x_1 \\ + a_3 \end{array} \left| x^{n-4} \ldots \begin{array}{l} + x_1^{n-1} \\ + a_1 x_1^{n-2} \\ + a_2 x_1^{n-3} \\ \vdots \\ + a_{n-2} x_1 \\ + a_{n-1}. \end{array} \right.$$

Aehnliche Ausdrücke erhält man für die übrigen Brüche, wenn man die hier vorkommende Wurzel x_1 nach und nach mit den übrigen Wurzeln x_2, $x_3 \ldots x_n$ vertauscht.

Addirt man alle auf diese Weise erhaltenen Gleichungen, so erhält man mittelst der oben angegebenen Bezeichnung:

$$f'(x) = n x^{n-1} \begin{array}{l} + s_1 \\ + n a_1 \end{array} \left| x^{n-2} \begin{array}{l} + s_2 \\ + a_1 s_1 \\ + n a_2 \end{array} \right| x^{n-3} \begin{array}{l} + s_3 \\ + a_1 s_2 \\ + a_2 s_1 \\ + n a_3 \end{array} \left| x^{n-4} \ldots \begin{array}{l} + s_{n-1} \\ + a_1 s_{n-2} \\ + a_2 s_{n-3} \\ \vdots \\ + a_{n-2} s_1. \\ + n a_{n-1}. \end{array} \right.$$

---

also

$$\frac{f(x+h)}{f(x)} = \left(1 + \frac{h}{x-x_1}\right)\left(1 + \frac{h}{x-x_2}\right) \ldots \left(1 + \frac{h}{x-x_n}\right);$$

aber

$$\frac{f(x+h)}{f(x)} = 1 + \frac{f'(x)}{f(x)} \frac{h}{1} + \frac{f''(x)}{f(x)} \frac{h^2}{1.2} + \ldots$$

Führt man die Multiplication auf der rechten Seite aus und vergleicht die Coefficienten der gleichhohen Potenzen von h, so erhält man

$$\frac{f'(x)}{f(x)} = \frac{1}{x-x_1} + \frac{1}{x-x_2} \ldots + \frac{1}{x-x_n},$$

$$\frac{1}{2} \frac{f''(x)}{f(x)} = \frac{1}{(x-x_1)(x-x_2)} + \frac{1}{(x-x_1)(x-x_3)} \ldots + \frac{1}{(x-x_{n-1})(x-x_n)}$$

u. s. w.

Auf der anderen Seite hat man:

$$f'(x) = n x^{n-1} + (n-1) a_1 x^{n-2} + (n-2) a_2 x^{n-3} \ldots + a_{n-1}; \quad (5)$$

da die für $f'(x)$ gefundenen Ausdrücke identisch sein müssen, folgt hieraus

$$\left.\begin{array}{l} s_1 + a_1 = 0, \\ s_2 + a_1 s_1 + 2 a_2 = 0, \\ s_3 + a_1 s_2 + a_2 s_1 + 3 a_3 = 0, \\ \vdots \\ s_{n-1} + a_1 s_{n-2} + a_2 s_{n-3} + \ldots a_{n-2} s_1 + (n-1) a_{n-1} = 0. \end{array}\right\} \quad (6)$$

Aus diesen Gleichungen findet man nach und nach

$$\left.\begin{array}{l} s_1 = -a_1, \\ s_2 = a_1^2 - 2 a_2, \\ s_3 = -a_1^3 + 3 a_1 a_2 - 3 a_3, \\ s_4 = a_1^4 - 4 a_1^2 a_2 + 4 a_1 a_3 + 2 a_2^2 - 4 a_4, \\ s_5 = -a_1^5 + 5 a_1^3 a_2 - 5 a_1^2 a_3 - 5 (a_2^2 - a_4) a_1 + 5 a_2 a_3 - 5 a_5. \\ \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots \end{array}\right\} (7)$$

Die gefundenen Formeln dienen nur zur Bestimmung von $s_1, s_2 \ldots s_{n-1}$. Um Formeln zur Berechnung von s_n, s_{n+1} u. s. w. zu finden, multiplicire man $f(x)$ mit x^m, wodurch man erhält

$$x^{n+m} + a_1 x^{n+m-1} + a_2 x^{n+m-2} \ldots + a_n x^m = 0,$$

eine Gleichung, welcher durch $x_1, x_2 \ldots x_n$ Genüge geleistet wird.

Setzt man nach und nach diese Werthe statt x ein und addirt dann die auf diese Weise erhaltenen Gleichungen, so erhält man

$$s_{n+m} + a_1 s_{n+m-1} + a_2 s_{n+m-2} + \ldots + a_n s_m = 0. \quad \ldots \quad (8)$$

Lässt man hierin m allmählig die Werthe $0, 1, 2 \ldots$ annehmen, erhält man (indem $s_0 = n$)

$$\left.\begin{array}{l} s_n + a_1 s_{n-1} + a_2 s_{n-2} \ldots + n a_n = 0, \\ s_{n+1} + a_1 s_n + a_2 s_{n-1} \ldots + a_n s_1 = 0, \\ s_{n+2} + a_1 s_{n+1} + a_2 s_n \ldots + a_n s_2 = 0, \\ \ldots\ldots\ldots \end{array}\right\} \quad \ldots\ldots \quad (9)$$

Diese Formeln dienen zur Berechnung von s_n, s_{n+1}, $s_{n+2}\dots$, wenn s_{n-1}, $s_{n-2}\dots$ durch die früheren Formeln gefunden worden sind.

Die gefundenen Formeln zeigen, dass die Summen der Potenzen der Wurzeln ganze Zahlen werden, wenn die Coefficienten es sind. Mit Rücksicht auf das folgende sei ferner bemerkt, dass alle gefundenen Gleichungen homogen sind, wenn man die Indices für jedes a und s den Grad bestimmen lässt. Ausserdem sieht man, dass die Coefficienten durch lineare Gleichungen bestimmt werden, sobald man

$$s_1, s_2 \dots s_n$$

kennt.

Kennt man s_p für n beliebige Werthe von p, geben die gefundenen Gleichungen ebenso viele Gleichungen zur Bestimmung der Coefficienten, wie Unbekannte vorhanden sind.

Die Bestimmung von s_{-p} wird auf die Bestimmung von s_p für eine andere Gleichung zurückgeführt, nämlich für die, welche aus der gegebenen durch Vertauschung von x mit $\frac{1}{x}$ gebildet wird; für diese hat man nämlich

$$S_p = \Sigma \left(\frac{1}{x_1}\right)^p = \Sigma x_1^{-p} = s_{-p}.$$

20. Man kann einen anderen Weg einschlagen, um die symmetrische Function s_p zu berechnen. Es ist nämlich

$$\frac{1}{x - x_p} = \frac{1}{x} + \frac{x_p}{x^2} + \frac{x_p^2}{x^3} + \dots\dots\dots \quad (10).$$

Diese Gleichung gilt für alle Wurzeln, wenn x grösser genommen wird als die grösste derselben, so dass die Reihe convergent wird; setzt man nun nach und nach für x_p alle Wurzeln der Gleichung ein und addirt, so erhält man mit Hülfe von 19 (2)

$$\frac{f'(x)}{f(x)} = \frac{n}{x} + \frac{s_1}{x^2} + \frac{s_2}{x^3} + \dots$$

oder

$$\frac{x f'(x)}{f(x)} = n + \frac{s_1}{x} + \frac{s_2}{x^2} + \dots\dots\dots \quad (11)$$

Entwickelt man nun die Grösse auf der linken Seite des Gleichheitszeichens in eine Reihe nach Potenzen von x mit negativen Exponenten, so erhält man für diese Grösse zwei Ausdrücke, welche gleich gross sind für alle Werthe von x über einer gewissen Grenze, und welche deshalb identisch sein müssen. Die durch die Division gefundenen Ausdrücke sind also eben die gesuchten Grössen s_1, s_2 . . . . .

Die Grösse $\frac{1}{x - x_1}$ kann auch für ein hinreichend kleines x in eine convergente Reihe nach Potenzen von x mit positiven Exponenten entwickelt werden; man erhält

$$\frac{1}{x - x_1} = -\left(\frac{1}{x_1} + \frac{x}{x_1^2} + \frac{x^2}{x_1^3} + \dots\right)$$

und daraus durch dasselbe Verfahren wie oben

$$-\frac{f'(x)}{f(x)} = s_{-1} + s_{-2}\,x + s_{-3}\,x^2 + \dots\dots\dots \quad (12)$$

wodurch s_{-1}, s_{-2}, s_{-3} u. s. w. gefunden werden, wenn der Bruch auf der linken Seite in eine Reihe mit positiven Exponenten für x entwickelt wird.

Man sieht leicht die Uebereinstimmung zwischen dem Verfahren, durch welches s_p aus s_{p-1}, $s_{p-2} \dots s_{p-n}$ mittelst 19 (9) gefunden wird, und dem Verfahren, durch welches, bei Entwicklung von Brüchen in recurrirende Reihen, jeder der Coefficienten aus den vorhergehenden gebildet wird. Die Glieder der Relationsscala sind eben die Coefficienten der Gleichung mit entgegengesetzten Vorzeichen.

Andre symmetrische Functionen.

21. Man nennt die gefundenen symmetrischen Functionen einförmig; zweiförmig sind die, deren bestimmendes Glied zwei Wurzeln enthält, dreiförmig die, bei denen das Glied drei Wurzeln enthält u. s. w. Bei den zweiförmigen hat also

das allgemeine Glied die Form $x_1^\alpha x_2^\beta$. Bildet man das Product $s_\alpha s_\beta$, so findet man darin dieselben Glieder wie in $\Sigma x_1^\alpha x_2^\beta$, und ausserdem die Glieder, welche durch Multiplication von Potenzen derselben Wurzel mit einander (x_1^α mit x_1^β u. s. w.) gebildet sind; man hat also

$$\Sigma x_1^\alpha x_2^\beta = s_\alpha s_\beta - s_{\alpha+\beta} \ldots\ldots\ldots\ldots (1).$$

Man sieht, dass die zweiförmigen Functionen rationale ganze Zahlen werden, wenn die Coefficienten es sind, und dass ihr Grad, wenn man der oben angegebenen Regel folgt, durch Addition der Exponenten gefunden wird.

Für $\alpha = \beta$ werden zwei und zwei Glieder gleich, da $x_1^\alpha x_2^\alpha = x_2^\alpha x_1^\alpha$. Da man nun bei der symmetrischen Function jedes dieser Glieder nur einmal mitnehmen darf, erhält man

$$\Sigma x_1^\alpha x_2^\alpha = \tfrac{1}{2}\left(s_\alpha^2 - s_{2\alpha}\right) \ldots\ldots\ldots\ldots (2).$$

Um die dreiförmige symmetrische Function $\Sigma x_1^\alpha x_2^\beta x_3^\gamma$ zu finden, multiplicire man (1) mit s_γ, woraus

$$s_\gamma \Sigma x_1^\alpha x_2^\beta = s_\alpha s_\beta s_\gamma - s_{\alpha+\beta} s_\gamma.$$

Die Glieder auf der linken Seite sind eben die, welche in der gesuchten Function vorkommen, aber ausserdem finden sich dort die Glieder, welche dadurch gebildet werden, dass ein Glied x_p^γ von s_γ mit den Gliedern des andern Factors, in welchen x_p auch vorkommt, multiplicirt wird; diese Glieder bilden die symmetrische Function

$$\Sigma x_1^{\alpha+\gamma} x_2^\beta + \Sigma x_1^\alpha x_2^{\beta+\gamma} = s_\beta s_{\alpha+\gamma} + s_\alpha s_{\beta+\gamma} - 2 s_{\alpha+\beta+\gamma},$$

und man erhält also

$$\Sigma x_1^\alpha x_2^\beta x_3^\gamma = s_\alpha s_\beta s_\gamma - s_\alpha s_{\beta+\gamma} - s_\beta s_{\alpha+\gamma} - s_\gamma s_{\alpha+\beta} + 2 s_{\alpha+\beta+\gamma} \; (3).$$

Falls zwei der Exponenten gleich gross sind, werden zwei und zwei Glieder gleich, falls alle drei Exponenten

gleich gross sind, werden je 6 Glieder unter einander gleich; man erhält deshalb

$$\Sigma x_1^{\alpha} x_2^{\alpha} x_3^{\gamma} = \tfrac{1}{2}\left(s^2_{\alpha} s_{\gamma} - 2 s_{\alpha} s_{\alpha+\gamma} - s_{2\alpha} s_{\gamma} + 2 s_{2\alpha+\gamma}\right) \quad . \; . \; (4)$$

und

$$\Sigma x_1^{\alpha} x_2^{\alpha} x_3^{\alpha} = \frac{1}{2.3}\left(s^3_{\alpha} - 3 s_{\alpha} s_{2\alpha} + 2 s_{3\alpha}\right) \quad . \; . \; . \; . \; . \; (5).$$

Auf diese Weise kann man fortfahren und dergestalt ist bewiesen, dass *jede symmetrische Function der Wurzeln eine rationale ganze Function der Coefficienten ist;* die Function ist homogen und ihr Grad wird durch Addition der Exponenten des bestimmenden Gliedes gefunden, wenn man a_p als vom p[ten] Grade betrachtet.

Andere Methode zur Berechnung der symmetrischen Functionen der Wurzeln.

22. Während Newton's Formeln mit verhältnissmässiger Leichtigkeit bei numerischen Gleichungen angewendet werden, giebt es andere Methoden, welche bei algebraischen Gleichungen mit Buchstabencoefficienten vorzuziehen sind. Solche sind von Waring und Cauchy gegeben; hier soll es indessen vorgezogen werden, eine Methode darzustellen, welche am nächsten mit der von Waring übereinstimmt, aber bequemer in ihrer Anwendung ist.

Der Bequemlichkeit wegen schreibe man die gegebene Gleichung

$$x^n - a_1 x^{n-1} + a_2 x^{n-2} - a_3 x^{n-3} + \ldots = 0; \quad . \; . \; . \; . \; . \; (1)$$

die symmetrische Function φ werde vom Grade α angenommen; dann sei

$$\varphi = A_{\alpha-n} a_n + A_{\alpha-n+1} a_{n-1} + \quad . \; . \; . \; . \; . \; . \; . \; . \; . \; (2),$$

worin das erste Glied aus allen den Gliedern zusammengesetzt ist, welche a_n enthalten, das zweite aus allen übrig gebliebe-

nen Gliedern, welche a_{n-1} enthalten, u. s. w. Der Index giebt überall den Grad an.

Da diese Gleichung, wenn a_n, a_{n-1} u. s. w. durch die Wurzeln ausgedrückt werden, eine Identität ist, kann man auf beiden Seiten des Gleichheitszeichens so viele Wurzeln gleich Null setzen, dass nur das letzte Glied auf der rechten Seite zurückbleibt; wenn dieses darauf gefunden ist, wird es auf die andere Seite hinübergebracht; man kann dann das Product der restirenden Wurzeln durch Division entfernen und auf dieselbe Weise fortfahren. Wie man oft diese Division vermeiden kann, wird sich am leichtesten zeigen lassen, wenn die Methode auf ein paar Beispiele angewendet wird.

Beisp. 1.

$$\Sigma x_1^3 x_2^2 x_3 = A_0 a_6 + A_1 a_5 + A_2 a_4 + A_3 a_3 \quad \ldots\ldots (3)$$

Im ersten Gliede erhält man a_6, da die Function vom 6ten Grade ist; ist die gegebene Function von einem niedrigeren Grade, so wird dieses Glied fortfallen; im letzten Gliede erhält man a_3, da die Function Null wird, wenn man alle Wurzeln mit Ausnahme von zweien gleich Null setzt.

Nun setze man

$$x_4 = x_5 = x_6 \ldots = 0,$$

dann ist

$$\Sigma x_1^3 x_2^2 x_3 = A_3 a_3, \quad \ldots\ldots\ldots\ldots (4)$$

wo die ursprünglichen Bezeichnungen beibehalten werden, aber daran erinnert wird, dass der höchste Index 3 ist. Hieraus erhält man, wenn man durch $x_1 x_2 x_3$ dividirt:

$$\Sigma x_1^2 x_2 = A_3 = \alpha_0 a_3 + \alpha_1 a_2 a_1; \quad \ldots\ldots\ldots (5)$$

in A_3 kommt a_1^3 nicht vor, da die Function Null werden muss, wenn zwei der Wurzeln gleich Null gesetzt werden.

Setzt man $x_3 = 0$, so erhält man

$$x_1 x_2 \Sigma x_1 = \alpha_1 a_2 a_1; \ \alpha_1 = 1,$$

und hierdurch aus (5)

$$\alpha_0 = \frac{\Sigma x_1^2 x_2 - a_1 a_2}{x_1 x_2 x_3}.$$

Da diese Gleichung identisch ist, kan man alle Wurzeln

gleich 1 setzen, wobei man nur die Anzahl der Glieder im Zähler zu bestimmen hat; dadurch erhält man

$$a_0 = 6 - 3 . 3 = -3$$

und hat nun, indem $x_p = 0$ für $p > 4$,

$$\Sigma x_1^3 x_2^2 x_3 = A_2 a_4 - 3 a_3^2 + a_1 a_2 a_3$$

oder

$$\frac{\Sigma x_1^3 x_2^2 x_3 + 3 a_3^2 - a_1 a_2 a_3}{x_1 x_2 x_3 x_4} = A_2 = \alpha_0 a_2 + \alpha_1 a_1^2,$$

worin die Coefficienten α_0 und α_1 gefunden werden sollen. Um das zu erreichen setzt man die drei Wurzeln gleich 1, die vierte gleich h, und sucht den Coefficienten für h^2, also im Zähler auf der linken Seite für h^3; in $\Sigma x_1^3 x_2^2 x_3$ benutzt man also nur die Glieder, in denen h den Exponenten 3 hat, und von diesen giebt es eben so viele, als es Möglichkeiten giebt, die beiden anderen in jedem Gliede vorkommenden Wurzeln zwischen den drei Wurzeln 1 herauszunehmen; hier kommt also der Coefficient 6; da nun ferner

$$a_3 = 1 + 3h; \; a_2 = 3 + 3h; \; a_1 = h + 3,$$

so erhält man

$$6 - 9 = \alpha_1 = -3,$$

und wenn man alle Wurzeln gleich 1 setzt:

$$24 + 48 - 96 = 6\alpha_0 - 3 . 16,$$

$$\alpha_0 = 4,$$

so dass nun

$$\frac{\Sigma x_1^3 x_2^2 x_3 - a_4 (4 a_2 - 3 a_1^2) + 3 a_3^2 - a_1 a_2 a_3}{x_1 x_2 x_3 x_4 x_5} = A_1 = \alpha a_1,$$

indem hier alle Wurzeln mit Ausnahme von 5 gleich Null gesetzt sind; setzt man diese 5 gleich 1, so erhält man

$$60 - 5 (4 . 10 - 3 . 25) + 3 . 10^2 - 5 . 10 . 10 = \alpha . 5,$$

$$\alpha = 7,$$

und endlich auf dieseselbe Weise $A_0 = -12$, so dass das gesuchte Resultat für alle Gleichungen wird

$$\Sigma x_1^3 x_2^2 x_3 = -12 a_6 + 7 a_5 a_1 + a_4 (4 a_2 - 3 a_1^2) - 3 a_3^2 + a_1 a_2 a_3.$$

Beisp. 2. Für die Gleichung

$$x^3 - a_1 x^2 + a_2 x - a_3 = 0$$

soll berechnet werden:

$$U = (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2.$$

Man hat

$$U = A_3 a_3 + A_4 a_2,$$

denn die folgenden Glieder müssen fehlen, da U Null wird, wenn zwei der Wurzeln gleich Null gesetzt werden. Für $x_3 = 0$ erhält man

$$x_1^2 x_2^2 (x_1 - x_2)^2 = A_4 a_2 = a_2^2 (-4 a_2 + a_1^2),$$

also

$$U = a_3 (\alpha_0 a_3 + \alpha_1 a_2 a_1 + \alpha_2 a_1^3) + a_2^2 (-4 a_2 + a_1^2).$$

Man setze hierin $x_1 = x_2 = 1$; $x_3 = h$ und suche die Coefficienten für h^4; dadurch erhält man

$$0 = \alpha_2 + 4; \ \alpha_2 = -4,$$

die Coefficienten für h^3 ergeben

$$2\alpha_1 - 24 - 12 = 0; \ \alpha_1 = 18,$$

während man, wenn man darauf alle Wurzeln gleich 1 setzt, $\alpha_0 = -27$ findet und also hat

$$U = -27 a_3^2 + 18 a_3 a_2 a_1 - 4 a_3 a_1^3 - 4 a_2^3 + a_2^2 a_1^2.$$

Sowohl in diesem wie in dem vorigen Beispiel wird das Resultat dasselbe, wenn man für die Gleichung die gewöhnliche Form mit positiven Coefficienten benutzt.

Allgemeine Formeln für s_p und a_p.

23. Mit Hülfe von Newton's Formeln kan man s_p berechnen, wenn die Coefficienten gegeben sind, und umgekehrt die Coefficienten, wenn $s_1, s_2 \ldots s_n$ gegeben sind; aber diese Berechnung verlangt die Auflösung eines Systems linearer Gleichungen. Durch die folgende Methode erhält man dagegen sofort explicite Ausdrücke für die gesuchten Grössen.

Es sei

$$(x-x_1)(x-x_2)\ldots(x-x_n) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n\,; \quad (1)$$

in dieser identischen Gleichung denke man sich x einen Werth beigelegt, der grösser ist als die grösste der Wurzeln, dann erhält man, wenn man durch x^n dividirt und den natürlichen Logarithmus nimmt

$$l\left(1-\frac{x_1}{x}\right)+l\left(1-\frac{x_2}{x}\right)+\ldots l\left(1-\frac{x_n}{x}\right)=l\left(1+\frac{a_1}{x}+\frac{a_2}{x^2}\ldots+\frac{a_n}{x^n}\right); \quad (2)$$

alle Glieder können hier in convergente Reihen entwickelt werden, wodurch man erhält

$$-\left(\frac{s_1}{x}+\frac{s_2}{2x^2}+\ldots\frac{s_p}{px^p}+\ldots\right)=\alpha-\frac{\alpha^2}{2}+\frac{\alpha^3}{3}\quad\frac{\alpha^4}{4}+\ldots, \quad (3)$$

indem

$$\alpha=\frac{a_1}{x}+\frac{a_2}{x^2}+\ldots+\frac{a_n}{x^n}.$$

Nun vergleicht man die Coefficienten für x^{-p} auf beiden Seiten; auf der linken Seite ist er $-\frac{s_p}{p}$; auf der rechten Seite ist das allgemeine Glied

$$\frac{(-1)^{k+1}}{k}\left(\frac{a_1}{x}+\frac{a_2}{x^2}+\ldots+\frac{a_n}{x^n}\right)^k,$$

wo wiederum das allgemeine Glied der Grösse in der Klammer zufolge der Polynomialformel gleich

$$\frac{(\beta_1+\beta_2+\ldots\beta_n)!}{\beta_1!\,\beta_2!\ldots\beta_n!}\,a_1^{\beta_1}\,a_2^{\beta_2}\,a_3^{\beta_3}\ldots a_n^{\beta_n}\,x^{-(\beta_1+2\beta_2+\ldots n\beta_n)}, \quad (4)$$

worin

$$\beta_1+\beta_2+\ldots\beta_n=k \;\ldots\ldots\ldots\ldots\ldots \quad (5)$$

Von diesen Gliedern werden hier nur die benutzt, für welche

$$\beta_1+2\beta_2+\ldots n\beta_n=p, \;\ldots\ldots\ldots\ldots \quad (6)$$

so dass die allgemeine Lösung wird:

$$s_p=\Sigma\frac{(-1)^{\beta_1+\beta_2+\ldots\beta_n}\,p\,(\beta_1+\beta_2+\ldots\beta_n-1)!}{\beta_1!\,\beta_2!\ldots\beta_n!}\,a_1^{\beta_1}\,a_2^{\beta_2}\ldots a_n^{\beta_n}, \quad (7)$$

wo $\beta_1, \beta_2 \dots \beta_n$ alle die positiven ganzen Werthe (Null eingerechnet) bekommen, welche (6) genügen.

Um einen expliciten Ausdruck für a_p zu bekommen, entwickle man aus (2)

$$1 + \frac{a_1}{x} + \frac{a_2}{x^2} + \dots \frac{a_p}{x^p} + \dots \frac{a_n}{x^n} = e^{-\left(\frac{s_1}{x} + \frac{s_2}{2x^2} + \dots\right)}$$

$$= 1 - \frac{\alpha}{1} + \frac{\alpha^2}{1.2} - \dots, \quad \dots \quad (8)$$

indem

$$\alpha = \frac{s_1}{x} + \frac{s_2}{2x^2} + \frac{s_3}{3x^3} + \dots$$

Hieraus erhält man nun durch ein Verfahren wie das obige:

$$a_p = \Sigma \frac{(-1)^{\beta_1 + \beta_2 + \dots \beta_p}}{\beta_1!\,\beta_2! \dots \beta_p!} \left(\frac{s_1}{1}\right)^{\beta_1} \left(\frac{s_2}{2}\right)^{\beta_2} \dots \left(\frac{s_p}{p}\right)^{\beta_p}, \quad . \quad (9)$$

worin

$$\beta_1 + 2\beta_2 + 3\beta_3 + \dots p\beta_p = p \quad \dots \dots \dots \quad (10).$$

Beispielsweise findet man hierdurch

$$\left.\begin{aligned} a_1 &= -s_1, \\ 2a_2 &= s_1^2 - s_2, \\ 2.3.a_3 &= -s_1^3 + 3s_1 s_2 - 2s_3, \\ 2.3.4.a_4 &= s_1^4 - 6s_1^2 s_2 + 8s_1 s_3 + 3s_2^2 - 6s_4, \\ 5!\,a_5 &= -s_1^5 + 10s_1^3 s_2 - 20s_1^2 s_3 - 15s_1 s_2^2 + 30s_1 s_4 \\ &\quad + 20s_2 s_3 - 24s_5, \end{aligned}\right\} \dots\dots \quad (11)$$

ebenso wie man es durch Anwendung von Newton's Formeln finden würde.

24. Wendet man (7) auf die Gleichung

$$x^2 - ax + b = 0 \quad \dots \dots \dots \dots \dots \quad (12)$$

an, so erhält man

$$s_p = \Sigma \frac{(-1)^\mu p (p - \mu - 1)!}{(p - 2\mu)!\,\mu!} a^{p-2\mu} b^\mu, \quad \dots \dots \quad (13)$$

worin μ nach und nach alle Werthe

0, 1, 2...

erhält, bis zu der grössten ganzen Zahl welche in $\frac{p}{2}$ ent-

halten ist. Der Ausdruck kann auch folgendermasssen geschrieben werden:

$$s_p = a^p - pa^{p-2}b + \frac{p(p-3)}{1.2}a^{p-4}b^2 \dots$$

$$+ (-1)^\mu \frac{p(p-\mu-1)(p-\mu-2)\dots(p-2\mu+1)}{1.2.3\dots\mu} a^{p-2\mu}b^\mu + \dots \quad (14)$$

Für die Gleichung

$$z^2 - zx + 1 = 0$$

erhält man

$$s_p = x^p - px^{p-2} + \frac{p(p-3)}{1.2}x^{p-4} - \dots$$

$$+ (-1)^\mu \frac{p(p-\mu-1)(p-\mu-2)\dots(p-2\mu+1)}{1.2.3\dots\mu} x^{p-2\mu} + \dots \quad (15)$$

ein Ausdruck, der später Verwendung finden wird.

Die Gleichung der quadrirten Wurzeldifferenzen.

25. Aus einer gegebenen Gleichung kann man eine neue Gleichung bilden, deren Wurzeln die Quadrate der Differenzen zwischen je zwei Wurzeln der gegebenen Gleichung sind; sind die Wurzeln der gegebenen Gleichung

$$x_1, x_2 \dots x_n,$$

werden also die Wurzeln der gesuchten Gleichung

$$(x_1 - x_2)^2, (x_1 - x_3)^2 \dots (x_{n-1} - x_n)^2,$$

und die Gleichung wird demgemäss vom Grade $\frac{n(n-1)}{2}$.

Diese Gleichung hat früher eine grosse Rolle in der Theorie der Gleichungen gespielt. Setzt man das letzte Glied derselben gleich Null, so erhält man die Bedingung dafür, dass die gegebene Gleichung ein Paar gleich grosser Wurzeln hat, da dies mit sich führen muss, dass eine der Wurzeln der Differenzengleichung Null wird. Hat die gegebene Gleichung

zwei Paare gleich grosser Wurzeln, z. B. $x_1 = x_2$, $x_3 = x_4$, so werden $(x_1 - x_2)^2$ und $(x_3 - x_4)^2$ Null, so dass die beiden letzten Glieder der Differenzengleichung fortfallen; giebt es drei Paare gleich grosser Wurzeln oder drei gleich grosse Wurzeln, so fallen die drei letzten Glieder fort u. s. w.

Die Gleichung der quadrirten Differenzen erhielt namentlich ihre Bedeutung dadurch, dass sie als Mittel diente um die Intervalle zu finden, innerhalb derer die Wurzeln einer gegebenen Gleichung einzeln belegen waren; später soll diese Anwendung besprochen werden und es soll dann gezeigt werden, wie dieselbe jetzt durch eine einfachere Methode ersetzt wird.

Um die Gleichung der quadrirten Differenzen zu bilden hat Lagrange die Potenzsummen S_1, $S_2 \ldots$ ihrer Wurzeln mit Hülfe der Werthe s_1, $s_2 \ldots$ der gegebenen Gleichung auf folgende Weise berechnet:

Durch Anwendung der Binomialformel hat man identisch:

$$(x - x_1)^{2p} + (x - x_2)^{2p} + \ldots (x - x_n)^{2p}$$
$$= n x^{2p} - \frac{2p}{1} x^{2p-1} s_1 + \frac{2p(2p-1)}{1.2} x^{2p-2} s_2 + \ldots;$$

setzt man hierin successive x_1, $x_2 \ldots x_3$ an Stelle von x und addirt, so wird

$$2S_p = n s_{2p} - \frac{2p}{1} s_{2p-1} s_1 + \frac{2p(2p-1)}{1.2} s_{2p-2} s_2 \ldots + n s_{2p},$$

oder, da die Glieder in gleichen Abständen von den Endpunkten der Reihe gleich sind,

$$S_p = n s_{2p} - \frac{2p}{1} s_{2p-1} s_1 + \ldots \pm \tfrac{1}{2} \frac{2p(2p-1)\ldots(p+1)}{1.2.3\ldots p} s_p^2 \quad \ldots (1)$$

Ist z. B. die gegebene Gleichung

$$x^3 + p x^2 + q x + r = 0,$$

so erhält man

$$S_1 = 3 s_2 - s_1^2$$
$$S_2 = 3 s_4 - 4 s_1 s_3 + 3 s_2^2$$
$$S_3 = 3 s_6 - 6 s_1 s_5 + 15 s_2 s_4 - 10 s_3^2$$

und daraus die Gleichung der quadrirten Differenzen

$$y^3 + Py^2 + Qy + R = 0,$$

worin

$$P = -2p^2 + 6q$$
$$Q = p^4 - 6p^2q + 9q^2$$
$$R = 4p^3r - p^2q^2 - 18pqr + 4q^3 + 27r^2.$$

Rationale Functionen der Wurzeln.

26. Eine rationale Function einer der Wurzeln x_1 der Gleichung n^{ten} Grades $f(x) = 0$ kann geschrieben werden

$$\frac{\varphi(x_1)}{\psi(x_1)}, \quad \ldots\ldots\ldots\ldots \quad (1)$$

worin φ und ψ rational sind; multiplicirt man Zähler und Nenner mit $\psi(x_2)\,\psi(x_3)\ldots\psi(x_n)$, erhält man

$$\varphi(x_1)\,\frac{\psi(x_2)\,\psi(x_3)\ldots\psi(x_n)}{\psi(x_1)\,\psi(x_2)\ldots\psi(x_n)}, \quad \ldots\ldots \quad (2)$$

wo der Nenner des Bruches eine symmetrische Function der Wurzeln der Gleichung ist und folglich rational durch die Coefficienten ausgedrückt werden kann; der Zähler ist eine symmetrische Function der Wurzeln der Gleichung

$$\frac{f(x)}{x - x_1} = 0, \quad \ldots\ldots\ldots\ldots \quad (3)$$

deren Coefficienten, wenn die Division ausgeführt wird, rationale Functionen von x_1 und den gegebenen Coefficienten sind. Der gegebene Ausdruck ist dadurch auf eine ganze algebraische Function von x_1 zurückgeführt; ist diese von höherem als dem $(n-1)^{ten}$ Grade, kann derselben die Form

$$f(x_1)\,Q + R$$

gegeben werden, worin R höchstens vom $(n-1)^{ten}$ Grade ist; da nun $f(x_1) = 0$, *kann also jede rationale Function einer Wurzel als eine ganze Function der Wurzel vom höchstens* $(n-1)^{ten}$ *Grade ausgedrückt werden.*

Enthält der gegebene Ausdruck mehrere Wurzeln x_1, x_2, $x_3 \ldots$, so bringe man denselben zuerst auf die hier angegebene Weise auf die Form

$$A_0 + A_1 x_1 + \ldots A_{n-1} x_1^{n-1},$$

wo die Coefficienten dann x_2, $x_3 \ldots$ enthalten. Jeden dieser Coefficienten behandelt man nun auf dieselbe Weise mit Rücksicht auf x_2 u. s. w. Zuletzt gelangt man dann zu einer ganzen Function der in dem gegebenen Ausdruck vorkommenden Wurzeln, und keine von diesen bekommt einen höheren Exponenten als $n-1$.

Beisp. In der Gleichung

$$x^3 + px^2 + qx + r = 0$$

kann eine rationale Function der Wurzel x_1 auf die Form

$$a + bx_1 + cx_1^2$$

gebracht werden, oder, wie es oft vorzuziehen ist, auf die Form

$$\frac{\alpha x_1 + \beta}{x_1 + \gamma}.$$

Diese Form erhält man, wenn man in der Identität

$$c^2 (x^3 + px^2 + qx + r) = (cx^2 + bx + a)(cx + pc - b) + \left[qc^2 - c(a + bp) + b^2\right] x + rc^2 - apc + ab$$

x_1 an die Stelle von x setzt, woraus, da die Grösse auf der linken Seite Null ist,

$$cx_1^2 + bx_1 + a = -\frac{\left[qc^2 - c(a + bp) + b^2\right] x_1 + rc^2 - apc + ab}{cx_1 + pc - b}.$$

Drittes Kapitel.

Ueber Elimination.

Elimination einer Grösse.

27. Zwei algebraische Gleichungen zwischen x und y, die eine vom m^{ten}, die andere vom n^{ten} Grade, können auf die Form

$$f(y) = a_0 y^m + a_1 y^{m-1} + a_2 y^{m-2} + \ldots + a_m = 0, \quad \ldots \quad (1)$$

$$F(y) = b_0 y^n + b_1 y^{n-1} + b_2 y^{n-2} + \ldots + b_n = 0, \quad \ldots \quad (2)$$

gebracht werden, worin a_p und b_p Functionen von x einzig vom p^{ten} Grade sind. Aus diesen Gleichungen können andere gebildet werden, denen von denselben Werthen von x und y Genüge geleistet wird, welche den beiden gegebenen Gleichungen genügen.

Um diese Werthe zu finden, sucht man im Allgemeinen zuerst eine Gleichung zu bilden, welche nur die eine Unbekannte enthält. Diese Gleichung wird die *Endgleichung* genannt, und dieselbe wird also gebildet, wenn man aus den beiden Gleichungen die eine Unbekannte fortschafft (eliminirt). Bildet man die Endgleichung in x, so wird diese alle Werthe bestimmen, welche x haben kann; jedem dieser Werthe wird im Allgemeinen nur ein Werth von y entsprechen, welcher

im Verein mit dem betrachteten Werthe von x beiden gegebenen Gleichungen genügt; jedem solchen Werthe von x entspricht also ein gewisser Factor ersten Grades, welcher beiden Gleichungen gemeinschaftlich ist. Die Aufgabe kann deshalb auch von einer anderen Seite betrachtet werden, indem die Endgleichung die Bedingung dafür ausdrückt, dass die beiden Polynome $f(y)$ und $F(y)$ einen gemeinschaftlichen Factor haben. Es sollen nun die wichtigsten Methoden gezeigt werden, deren man sich bedient, um die Endgleichung zu bilden.

Anwendung symmetrischer Functionen.

28. Die Gleichung $F(y) = 0$ ist vom n^{ten} Grade mit Bezug auf y und hat also n Wurzeln, welche Functionen von x sind; diese können allgemein nicht gefunden werden, aber man kann sie durch $y_1, y_2 \ldots y_n$ bezeichnen. Für jeden der gesuchten Werthe von x soll wenigstens einer dieser Werthe der Gleichung $f(y) = 0$ genügen; die nothwendige und ausreichende Bedingung hierfür kann

$$f(y_1)\, f(y_2) \ldots f(y_n) = 0 \;\ldots\ldots\ldots\ldots \;(1)$$

geschrieben werden, indem dieser Gleichung genügt und zwar nur genügt wird, wenn einer der Factoren der linken Seite Null ist. Da $y_1, y_2 \ldots y_n$ symmetrisch in dieser Gleichung auftreten, können sie durch Anwendung der Theorie der symmetrischen Functionen fortgeschafft werden, indem man für sie Functionen von $b_1, b_2 \ldots b_n$, also von x allein, einführt. Die auf solche Weise gebildete Gleichung enthält dann alleine x und ist folglich die gesuchte Endgleichung.

Man kann leicht zeigen, dass diese Gleichung höchstens vom Grade mn wird. $f(y)$ ist nämlich homogen vom m^{ten} Grade, wenn man b_p als vom p^{ten} Grade betrachtet. Nimmt man $y_1, y_2 \ldots$ als vom ersten Grade an, so wird also $f(y_1)\, f(y_2) \ldots f(y_n)$ homogen vom Grade mn; nun sind alle Formeln, welche in der Theorie der symmetrischen Functionen

angewendet werden, homogen, wenn man die Wurzeln vom erstem Grade sein lässt und b_p vom Grade p; also wird die Endgleichung in x homogen vom mn^{ten} Grade sein, wenn man die Indices der darin vorkommenden Coefficienten a und b den Grad bestimmen lässt. In Wirklichkeit geben diese Indices indessen nur den höchsten Exponenten von x in den durch a und b bezeichneten ganzen Functionen von x an. Wird also x eingeführt, so bleibt der gefundene Ausdruck nicht mehr homogen, aber der höchste Exponent, mit welchem x vorkommen kann, ist mn. Der Umstand, dass b_0 in den Coefficienten von F(y) als Nenner auftritt, übt keinen Einfluss auf den Grad aus, da b_0 weder x noch y enthält.

Man sieht also, dass *die Endgleichung höchstens vom mn^{ten} Grade wird.* Sind die gegebenen Gleichungen vollständig und allgemein, d. h. kommen alle möglichen Glieder vor mit ganz willkührlichen, gegenseitig von einander unabhängigen Coefficienten, so muss der Grad genau mn sein; denn betrachtet man im Besonderen die Gleichungen

$$y = x^m;\ x = y^n, \qquad (2)$$

so erhält man eine Endgleichung von mn^{ten} Grade:

$$x^{mn} = x, \qquad (3)$$

und dieser Fall muss in dem allgemeinen mit einbegriffen sein, wenn nicht eine fremde Wurzel eingeführt ist; das ist aber nicht der Fall, denn ist x_1 eine der Wurzeln in (3), so giebt die erste Gleichung (2)

$$y_1 = x_1^m,$$

wodurch die zweite Gleichung (2)

$$x_1 = x_1^{mn}$$

wird; daraus geht hervor, dass alle Wurzeln von (3) Lösungen von (2) geben. Es ist also erwiesen, dass

zwei allgemeine Gleichungen vom m^{ten} und n^{ten} Grade auf eine Endgleichung vom mn^{ten} Grade führen.

29. Werden x und y als Coordinaten eines rechtwinkligen Coordinatensystems aufgefasst, so gehören die gegebenen Gleichungen zwei Curven der m^{ten} und n^{ten} Ordnung an, und ihre Wurzeln bestimmen die Durchschnittspunkte.

Zwei allgemeine Curven der m^{ten} und n^{ten} Ordnung haben also mn Durchschnittspunkte. In speciellen Fällen kann die Endgleichung von niedrigerem Grade sein. Geht man von dem allgemeinen Fall aus, und lässt man die Coordinaten continuirlich in die übergehen, welche in dem besonderen Fall vorkommen, so werden gleichzeitig die Cofficienten der höchsten Potenzen von x in der Endgleichung sich Null nähern, und ebenso viele Wurzeln werden gleichzeitig ohne Grenze wachsen (was man leicht sieht, wenn man x mit $\frac{1}{x}$ vertauscht). Man kann deshalb sagen, dass es immer mn Durchschnittspunkte oder mn zusammengehörige Wurzeln giebt, wenn man die unendlich fernen Durchschnittspunkte oder die unendlichen Wurzeln mitzählt. Diese Betrachtungsweise, welche dem Satze über die Anzahl der Durchschnittspunkte allgemeine Gültigkeit verleiht, wird mit grossem Vortheil in der neueren Geometrie angewendet.

Beisp. Die allgemeinen Gleichungen zweiten Grades sind

$$f(y) = a_0 y^2 + a_1 y + a_2 = 0$$

$$F(y) = b_0 y^2 + b_1 y + b_2 = 0$$

Hieraus erhält man für $f(y_1) f(y_2)$

$$a_0^2 y_1^2 y_2^2 + a_0 a_1 y_1 y_2 (y_1 + y_2) + a_1^2 y_1 y_2 + a_0 a_2 (y_1^2 + y_2^2) \\ + a_1 a_2 (y_1 + y_2) + a_2^2,$$

worin

$$y_1 y_2 = \frac{b_2}{b_0};\ y_1 + y_2 = -\frac{b_1}{b_0};\ y_1^2 + y_2^2 = \left(\frac{b_1}{b_0}\right)^2 - \frac{2 b_2}{b_0}.$$

Methode von Labatie.

30. Es seien $V_1 = 0$ und $V_2 = 0$ die gegebenen Gleichungen in x und y, geordnet wie vorhin, wo V_2 vom niedrigsten Grade (n) mit Beziehung auf y ist. Falls V_1 und V_2 einen gemeinschaftlichen Factor haben sollten, wird angenommen, derselbe sei durch Division entfernt; ausser der endlichen Anzahl von Lösungen, welche weiter unten bestimmt werden, wird dann den Gleichungen durch alle solche Werthe von x und y genügt, welche den gemeinschaftlichen Factor gleich Null machen.

Nun verfährt man wie beim Aufsuchen des grössten gemeinschaftlichen Factors für V_1 und V_2; dadurch gelangt man zuletzt zu einem Rest, welcher nur x enthält; wird dieser gleich Null gesetzt, so hat man die Endgleichung, denn diese Gleichung drückt eben die Bedingung dafür aus, dass V_1 und V_2 einen gemeinschaftlichen Factor haben. Die Sache verlangt indessen eine genauere Untersuchung, denn es können Wurzeln eingeführt oder fortgeschafft werden, indem man bei Ausführung der Rechnung gewisse Factoren einführt oder fortwirft um Brüche zu vermeiden. Diese Factoren sind Functionen von x allein; die Factoren, welche in die Dividenden eingeführt werden, sollen mit u bezeichnet werden, diejenigen, welche aus den Divisoren fortdividirt werden, mit v, die Quotienten mit Q; dann hat man zuerst

$$u_1 V_1 = Q_1 V_2 + V_3 v_1; \; \ldots\ldots\ldots\ldots \; (1).$$

man sieht hieraus, dass die beiden Systeme von Gleichungen

$$\begin{matrix} u_1 V_1 = 0 \\ V_2 = 0 \end{matrix} \quad \text{und} \quad \begin{matrix} V_2 = 0 \\ V_3 v_1 = 0 \end{matrix} \; \ldots\ldots\ldots\ldots \; (2)$$

dieselben endlichen Lösungen haben, da alle zusammengehörigen endlichen Werthe, welche dem einen System genügen, auch dem anderen System genügen müssen. Giebt es mehrfache Lösungen, muss man diese auch aus den beiden Systemen gleich oft finden; denn man kann die Systeme als specielle Fälle allgemeinerer Gleichungen betrachten, für

welche es keine mehrfachen Lösungen giebt; es müssen dann, indem man zu den gegebenen Gleichungen übergeht, gleichzeitig beide Systeme in denselben zusammengehörigen Wurzeln übereinstimmen.

Das hier gesagte gilt nur für endliche Wurzeln; die beiden Systeme brauchen nicht dieselben unendliche Wurzeln zu haben; so hat das System

$$x^2 + y^2 + ax + by + c = 0,$$

$$x^2 + y^2 + a_1 x + b_1 y + c_1 = 0$$

zwei zusammengehörige unendliche Wurzeln, während die eine von diesen Gleichungen in Verbindung mit

$$(a - a_1) x + (b - b_1) y + c - c_1 = 0$$

keine unendlichen Wurzeln hat. Von den unendlichen Wurzeln soll vorläufig abgesehen werden.

Die beiden Systeme von Gleichungen in (2) können auch geschrieben werden:

$$\left.\begin{matrix} u_1 = 0 \\ V_2 = 0 \end{matrix}\right\} \quad \left.\begin{matrix} V_1 = 0 \\ V_2 = 0 \end{matrix}\right\} \quad \text{und} \quad \left.\begin{matrix} v_1 = 0 \\ V_2 = 0 \end{matrix}\right\} \quad \left.\begin{matrix} V_2 = 0 \\ V_3 = 0 \end{matrix}\right\} \quad \ldots \quad (3)$$

diese Systeme sollen mit 1, 2, 3 und 4 bezeichnet werden.

Hieraus ist ersichtlich, dass man, wenn man das gegebene System 2 durch 4 ersetzt, von fremden Lösungen diejenigen einführt, welche dem System 1 angehören, während man die fortgeworfen hat, welche dem System 3 angehören. Falls nun u_1 und v_1 einen gemeinschaftlichen Factor d_1 haben, kann man diesen aus den beiden Ausdrücken durch Division entfernen, da derselbe an beiden Stellen mit $V_2 = 0$ combinirt werden soll, so dass dieselben ihm entsprechenden Wurzeln durch Division mit v_1 fortgeschafft und durch Multiplication mit u_1 eingeführt werden. Auf die Weise wird das gegebene System ersetzt durch

$$\left.\begin{matrix} \frac{v_1}{d_1} = 0 \\ V_2 = 0 \end{matrix}\right\} \quad \text{und} \quad \left.\begin{matrix} V_2 = 0 \\ V_3 = 0 \end{matrix}\right\} \quad \ldots\ldots\ldots\ldots \quad (4)$$

indem die hierdurch eingeführten fremden Lösungen bestimmt werden durch

$$\left.\begin{array}{l}\frac{v_1}{d_1}=0\\ V_2=0\end{array}\right\}\ldots\ldots\ldots\ldots\ldots\ldots (5)$$

Nun wird das System $V_2 = 0$, $V_3 = 0$ auf dieselbe Weise behandelt wie das ursprüngliche System und dergestalt wird fortgefahren, bis man zur Endgleichung gelangt, indem man beständig Rücksicht nimmt auf die ausgeschiedenen Systeme und auf die Systeme, welche die eingeführten fremden Wurzeln bestimmen. Um die Endgleichung vollständig zu bekommen, muss man sie also mit $\frac{v_1}{d_1}$ und den analogen Ausdrücken multipliciren, und darauf $\frac{u_1}{d_1}$ und die analogen Ausdrücke durch Division entfernen. Indessen muss, wenn es sich um vollständige Auflösung der Gleichungen handelt, daran erinnert werden, dass die hinzugefügten und fortgeschafften Wurzeln eine andere Rolle spielen als die übrigen, da die entsprechenden Werthe von y aus verschiedenen Gleichungen gefunden werden; dergestalt soll $\frac{v_1}{d_1} = 0$ mit $V_2 = 0$ combinirt werden, während hingegen eine analoge Gleichung $\frac{v_p}{d_p} = 0$ mit einer Gleichung $V_{p+1} = 0$, die der Gleichung $V_2 = 0$ analog ist, combinirt werden muss; es soll nunmehr gezeigt werden, wie man hier die Lösung vereinfachen kann.

31. Es sind nur die gemeinschaftlichen Factoren von einem u und einem v fortdividirt worden, wenn sie denselben Index hatten, weil man nur in diesem Falle $u = 0$ und $v = 0$ mit derselben Gleichung combiniren soll; indessen lässt sich folgender Satz beweisen:

Wenn ein u und ein folgendes v, z. B. u_2 und v_4, einen gemeinschaftlichen Factor $x-a$ enthalten, welcher nicht Factor von irgend einem zwischenliegenden u oder v ist, so kann das

System $x - \alpha = 0$, $V_3 = 0$ ersetzt werden durch das System $x - \alpha = 0$, $V_5 = 0$.

Betrachtet man nämlich die Gleichungen

$$\left.\begin{aligned} u_2 V_2 &= Q_2 V_3 + V_4 v_2 \\ u_3 V_3 &= Q_3 V_4 + V_5 v_3 \\ u_4 V_4 &= Q_4 V_5 + V_6 v_4 \end{aligned}\right\}, \quad \ldots\ldots\ldots\ldots (6)$$

so sieht man, dass $x = \alpha$ und die Werthe von y, welche $u_2 = 0$ und $V_3 = 0$ genügen, auch $V_4 = 0$ und $V_5 = 0$ genügen (da sie nicht v_2 oder v_3 zu Null machen), und umgehrt, dass die Werthe, welche $v_4 = 0$ und $V_5 = 0$ genügen, auch $V_3 = 0$ genügen. Es ist also gleichgültig, ob die gemeinschaftlichen Wurzeln in $u_2 = 0$ und $v_4 = 0$ mit $V_3 = 0$ oder mit $V_5 = 0$ combinirt werden, und man wird also (abgesehen von unendlich grossen Wurzeln) keinen Fehler begehen, wenn man die gemeinschaftlichen Factoren von u_2 und v_4 fortdividirt. Es kann also im Allgemeinen jeder Factor, der durch Multiplication mit einem u eingeführt wird, wieder fortgeschafft werden, sobald man ihn das erste Mal darauf in einem v antrifft.

Hat man beispielsweise in u_2 den Factor $x - \alpha_1$, und in u_3 den Factor $x - \alpha_2$ eingeführt, so kann man also diese Factoren fortschaffen, wenn man sie hinterher zum ersten Male in einem v antrifft; da dieses gilt, wie gering auch der Unterschied zwischen α_1 und α_2 sein mag, so muss es auch gelten für $\alpha_1 = \alpha_2$; wenn derselbe Factor mehrere Male eingeführt wird, kann man ihn also ebenso oft fortschaffen, sobald man ihn in einem v antrifft.

Man übersieht nun leicht, welche Gleichungen aufzulösen sind. Zuerst hat man von fremden Factoren $\frac{u_1}{d_1}$, darauf durch die nächste Multiplication $\frac{u_1 u_2}{d_1}$; von diesen werden diejenigen durch Division entfernt, welche sich in v_2 finden; werden diese d_2 genannt, so bleiben $\frac{u_1 u_2}{d_1 d_2}$ zurück und nach

der Multiplication $\frac{u_1 u_2 u_3}{d_1 d_2}$, von welchen d_3, welcher in v_3 vorkommt, entfernt wird u. s. w. Die gegebenen Gleichungen werden also durch folgende Systeme ersetzt:

$$\begin{matrix} \frac{v_1}{d_1}=0 \\ V_2=0 \end{matrix} ; \quad \begin{matrix} \frac{v_2}{d_2}=0 \\ V_3=0 \end{matrix} ; \quad \begin{matrix} \frac{v_3}{d_3}=0 \\ V_4=0 \end{matrix} ; \quad \ldots \quad \begin{matrix} \frac{v_{n-1}}{d_{n-1}}=0 \\ V_n=0 \end{matrix} , \quad \ldots\ldots \quad (7)$$

welche, abgesehen von den unendlichen Wurzeln, *nur die richtigen Lösungen liefern, und zwar alle richtigen Lösungen und jede derselben die richtige Anzahl Male.* Die eingeführten fremden Factoren müssen also alle, so weit es nicht schon früher geschehen ist, aus der Endgleichung fortdividirt werden können; der letzte Rest ist $V_{n+1} v_{n-1}$, worin indessen $V_{n+1} = 1$, da dieser Rest y nicht enthält; die Endgleichung ist also $v_{n-1} = 0$, aus der alle nicht schon früher fortgeschafften fremden Factoren d_{n-1} durch Division entfernt werden. Da V_n im Allgemeinen mit Bezug auf y vom ersten Grade ist, liefert das letzte System alle die zusammengehörigen Wurzeln, bei denen einem Werthe von x e i n Werth von y entspricht; das vorletzte alle die zusammengehörigen Wurzeln, bei denen einem Werthe von x zwei Werthe von y entsprechen u. s. w. Da solche zusammengehörige Wurzeln nur bei besonderen Gleichungen vorkommen können, erhält man das letzte System allein, wenn die gegebenen Gleichungen allgemeine sind. Die Endgleichung, welche man dadurch erhält, dass man den Rest gleich Null setzt, wird also von einem zu hohen Grade sein, da man aus derselben durch Division alle die Factoren muss entfernen können, welche nach und nach eingeführt sind um Brüche zu vermeiden. Auf solche Weise würden zwei allgemeine Gleichungen 3ten Grades zu einem Rest vom 11ten Grade führen, da man zwei Mal mit einem Factor ersten Grades oder mit einem Factor zweiten Grades hat multipliciren müssen. Man führt gewiss bei der letzten Division einen Factor vom 4ten Grade ein, aber dieser spielt keine Rolle, da, wie man leicht sieht, keine endlichen Wurzeln durch denselben eingeführt werden.

Ist die Zahl der zusammengehörigen Wurzeln kleiner, als sie nach dem allgemeinen Satze sein müsste, so sind die fehlenden Werthe von x unendlich. Eine genauere Untersuchung dieser hat wesentliche Bedeutung in der Geometrie; hier soll indessen darüber hinweg gegangen werden.

Beisp.

$$V_1 = y^3 + 2xy^2 + (2x^2 - 4x)y + x^2 - 4 = 0.$$

$$V_2 = y^2 + 2xy + 2x^2 - 5x + 2 = 0.$$

Aus dem ersten Reste wird $x-2$ durch Division entfernt und derselbe dann mit V_2 combinirt. Der zweite Divisor wird $y+x+2$ und giebt den Rest x^2-5x+6. Man erhält also die beiden Systeme

$$\begin{matrix} x = 2 \\ y^2 + 2xy + 2x^2 - 5x + 2 = 0 \end{matrix}; \quad \begin{matrix} x^2 - 5x + 6 = 0 \\ y + x + 2 = 0 \end{matrix},$$

also

$$\begin{matrix} x = 2 \\ y = 0 \end{matrix}; \quad \begin{matrix} x = 2 \\ y = -4 \end{matrix}; \quad \begin{matrix} x = 2 \\ y = -4 \end{matrix}; \quad \begin{matrix} x = 3 \\ y = -5 \end{matrix}.$$

Da man eine Endgleichung vom 6ten Grade erwarten sollte, sind die zwei Werthe von x unendlich. Betrachtet man die beiden Curven, welche durch die beiden Gleichungen repräsentirt werden, so sieht man, dass sie zwei unendlich ferne Durchschnittspunkte haben; von den vier übrigen Durchschnittspunkten fallen zwei in einem Berührungspunkte zusammen.

Euler's Methode.

32. Die beiden Gleichungen seien

$$\left.\begin{aligned} U &= a_0 y^m + a_1 y^{m-1} + a_2 y^{m-2} + \ldots + a_m = 0 \\ V &= b_0 y^n + b_1 y^{n-1} + b_2 y^{n-2} + \ldots + b_n = 0 \end{aligned}\right\} \quad \ldots\ldots (1)$$

Falls die beiden Polynome U und V für einen gewissen

Werth von x einen gemeinschaftlichen Factor φ von p^{ten} Grade haben, nämlich

$$\varphi = \alpha_0 y^p + \alpha_1 y^{p-1} + \ldots \alpha_p \quad \ldots\ldots\ldots\ldots (2)$$

so müssen, wenn

$$\frac{U}{\varphi} = M; \ \frac{V}{\varphi} = N, \quad \ldots\ldots\ldots\ldots\ldots (3)$$

die beiden Polynome

NU und MV

für diesen Werth von x identisch werden. N muss hier vom $(n-p)^{ten}$ Grade, M vom $(m-p)^{ten}$ Grade sein. Man multiplicire deshalb U und V mit Polynomen vom beziehungsweise $(n-p)^{ten}$ und $(m-p)^{ten}$ Grade mit unbestimmten Coefficienten, und setze die Coefficienten der gleichhohen Potenzen von y in den beiden Producten unter einander gleich. Aus den hierdurch gebildeten Gleichungen, welche vom ersten Grade sind, werden die unbestimmten Coefficienten eliminirt; die dadurch erhaltenen Gleichungen zwischen den Coefficienten von U und V drücken dann die nothwendigen und ausreichenden Bedingungen dafür aus, dass U und V einen gemeinschaftlichen Factor vom p^{ten} Grade haben.

Es sei

$$\left.\begin{array}{l} N = r_0 y^{n-p} + r_1 y^{n-p-1} + \ldots + r_{n-p} \\ M = t_0 y^{m-p} + t_1 y^{m-p-1} + \ldots + t_{m-p} \end{array}\right\} ; \quad \ldots\ldots (4)$$

dann würde man $m + n - 2p$ unbestimmte Coefficienten und durch Vergleichung der beiden Producte $m + n - p$ Gleichungen erhalten; nach Elimination der unbestimmten Coefficienten hat man dann p Bedingungsgleichungen. Wenn diesen genügt wird, hat man identisch

$$NU = MV,$$

und hieraus geht hervor, dass die n Factoren von V sich alle in NU finden müssen, und dass also wenigstens p von diesen in U vorkommen müssen, da N nur vom $(n-p)^{ten}$ Grade ist.

Für $p=1$ erhält man nur eine Bedingungsgleichung, welche die gesuchte Endgleichung ist.

Eine allgemeine Form für den gemeinschaftlichen Factor kann man erhalten, wenn man M und N beide um einen Grad niedriger nimmt als oben, und darauf die Cofficienten so bestimmt, dass die höchsten Potenzen von y aus der Differenz der beiden Producte fortfallen; dadurch erhält man nämlich, wenn die angewendeten Factoren mit N_1 und M_1 bezeichnet werden:

$$N_1 U - M_1 V = \alpha_0 y^p + \alpha_1 y^{p-1} + \ldots + \alpha_p, \quad \ldots\ldots (5)$$

woraus hervorgeht, dass der gemeinschaftliche Factor von U und V auch ein Factor der rechten Seite ist; sind nun die Bedingungen dafür erfüllt, dass ein Factor vom p^{ten} Grade vorhanden ist, so muss das Polynom auf der rechten Seite selbst dieser Factor sein.

Beisp.

$$U = y^3 + a_1 y^2 + a_2 y + a_3 = 0,$$
$$V = y^3 + b_1 y^2 + b_2 y + b_3 = 0.$$

Setzt man

$$(y^2 + \alpha_1 y + \alpha_2) U = (y^2 + \beta_1 y + \beta_2) V,$$

so erhält man durch Vergleichung der Coefficienten:

$$\begin{aligned} \alpha_1 + a_1 &= \beta_1 + b_1, \\ \alpha_2 + a_1 \alpha_1 + a_2 &= \beta_2 + b_1 \beta_1 + b_2, \\ a_1 \alpha_2 + a_2 \alpha_1 + a_3 &= b_1 \beta_2 + b_2 \beta_1 + b_3, \\ a_2 \alpha_2 + a_3 \alpha_1 &= b_2 \beta_2 + b_3 \beta_1, \\ a_3 \alpha_2 &= b_3 \beta_2. \end{aligned}$$

Die Elimination von α_1, α_2, β_1 und β_2 giebt die Endgleichung

$$\begin{vmatrix} 1 & 0 & 1 & 0 & a_1 - b_1 \\ a_1 & 1 & b_1 & 1 & a_2 - b_2 \\ a_2 & a_1 & b_2 & b_1 & a_3 - b_3 \\ a_3 & a_2 & b_3 & b_2 & 0 \\ 0 & a_3 & 0 & b_3 & 0 \end{vmatrix} = 0.$$

Um einen allgemeinen Ausdruck für den gemeinschaftlichen Factor zu bekommen setze man

$$(y + \alpha_1) U - (y + \beta_1) V = my + n;$$

daraus erhält man

$$
\begin{aligned}
\alpha_1 + a_1 &= \beta_1 + b_1, \\
\alpha_1 a_1 + a_2 &= \beta_1 b_1 + b_2, \\
\alpha_1 a_2 + a_3 &= \beta_1 b_2 + b_3 + m, \\
\alpha_1 a_3 &= \beta_1 b_3 + n,
\end{aligned}
$$

wo α_1 und β_1 durch die beiden ersten Gleichungen bestimmt und in die beiden letzten eingesetzt werden.

Sucht man die Bedingungen dafür, dass ein gemeinschaftlicher Factor vom 2ten Grade vorhanden ist, so erhält man dieselben Gleichungen, wie wenn man oben $m = n = 0$ setzt. Die beiden Bedingungsgleichungen erhält man dann dadurch, dass man α_1 und β_1 zweimal zwischen drei von den vier Gleichungen eliminirt; man pflegt unter der Bezeichnung

$$
\begin{vmatrix}
1 & a_1 & a_2 & a_3 \\
1 & b_1 & b_2 & b_3 \\
a_1 - b_1 & a_2 - b_2 & a_3 - b_3 & 0
\end{vmatrix} = 0
$$

alle die Gleichungen zu verstehen, welche man erhält, wenn man drei (die Anzahl der Zeilen) beliebige Colonnen behält und die übrigen fortwirft; hierdurch werden dann eben die gesuchten Bedingungen ausgedrückt, da eine so gebildete Determinante dieselbe ist, welche durch Elimination zwischen drei der Gleichungen gebildet wird. Von den vier Determinanten, welche hier gebildet werden können, sind indessen nur zwei von einander unabhängig. Sind die beiden durch diese ausgedrückten Bedingungen erfüllt, so erhält man die allgemeine Form für den gemeinschaftlichen Factor zweiten Grades, wenn man y^3 aus den gegebenen Gleichung eliminirt; dieselbe wird

$$(a_1 - b_1)\, y^2 + (a_2 - b_2)\, y + a_3 - b_3.$$

Sylvester's Methode.

33. Diese Methode ist im Wesentlichen dieselbe wie die vorhergehende. Sie besteht darin, dass man die gegebenen

Gleichungen mit y, y^2, y^3 ... multiplicirt, bis man beide in Gleichungen vom $(m+n-1)^{ten}$ Grade umgewandelt hat. Dadurch erhält man $m+n$ Gleichungen, zwischen welchen man y, y^2, y^3 ... y^{m+n-1}, welche als von einander unabhängige Unbekannte betrachtet werden, und mit Rücksicht auf welche also alle Gleichungen linear sind, eliminirt. Auf die Weise erhält man für die beiden eben behandelten Gleichungen

$$\begin{aligned}
y^3 + a_1 y^2 + a_2 y + a_3 &= 0,\\
y^4 + a_1 y^3 + a_2 y^2 + a_3 y &= 0,\\
y^5 + a_1 y^4 + a_2 y^3 + a_3 y^2 &= 0,\\
y^3 + b_1 y^2 + b_2 y + b_3 &= 0,\\
y^4 + b_1 y^3 + b_2 y^2 + b_3 y &= 0,\\
y^5 + b_1 y^4 + b_2 y^3 + b_3 y^2 &= 0,
\end{aligned}$$

und hieraus die Endgleichung

$$\begin{vmatrix}
0 & 0 & 1 & a_1 & a_2 & a_3\\
0 & 1 & a_1 & a_2 & a_3 & 0\\
1 & a_1 & a_2 & a_3 & 0 & 0\\
0 & 0 & 1 & b_1 & b_2 & b_3\\
0 & 1 & b_1 & b_2 & b_3 & 0\\
1 & b_1 & b_2 & b_3 & 0 & 0
\end{vmatrix} = 0.$$

Diese Gleichung wird identisch mit der oben gefundenen, wenn man die dritte Zeile mit derjenigen vertauscht, welche man erhält, wenn man die sechste Zeile von der dritten subtrahirt, und wenn man darauf die sechste Zeile und die erste Colonne auslöscht.

Lässt man oben die dritte und sechste Gleichung aus, so erhält man

$$\begin{vmatrix}
0 & 1 & a_1 & a_2 & a_3\\
1 & a_1 & a_2 & a_3 & 0\\
0 & 1 & b_1 & b_2 & b_3\\
1 & b_1 & b_2 & b_3 & 0
\end{vmatrix} = 0,$$

wodurch die beiden Bedingungen für einen gemeinschaftlichen Factor zweiten Grades gegeben sind u. s. w.

34. Das Resultat der geführten Untersuchungen über zwei Gleichungen mit zwei Unbekannten ist also folgendes:

Sind die beiden Gleichungen vom m^{ten} und n^{ten} Grade, so wird die Endgleichung im Allgemeinen vom mn^{ten} Grade;

in speciellen Fällen kann der Grad niedriger werden, indem das Vorhandensein eines gemeinschaftlichen Factors in den beiden Polynomen den Rest identisch gleich Null macht, oder unendliche Wurzeln die höchsten Potenzen der Unbekannten zum Wegfall bringen. Jedem durch die Endgleichung bestimmten Werthe von x entspricht im Allgemeinen nur ein Werth von y, der durch eine Gleichung, von der Form

$$Ay + B = 0$$

bestimmt wird. Für die Werthe von x, durch welche sowohl A als B zu Null werden, wird diese Gleichung unbrauchbar; y bekommt zwei Werthe, welche durch eine Gleichung von der Form

$$A_1 y^2 + B_1 y + C_1 = 0$$

bestimmt werden, es sei denn dass

$$A_1 = B_1 = C_1 = 0,$$

da y im solchem Falle drei Werthe erhält u. s. w.

Diese Resultate treten besonders deutlich hervor bei Labatie's Methode, bei der alle die Ausdrücke, welche man nöthig hat, um Bedingungsgleichungen oder Factoren zu bilden, in den Zwischenrechnungen gefunden werden; diese Methode ist deshalb sicher bei numerischen Gleichungen vorzuziehen, während vielleicht die Determinantenform, unter welcher die Resultate bei Euler's oder Sylvester's Methode erscheinen, bewirkt, dass diese vorgezogen werden müssen, wo es mehr auf ein leicht übersichtliches Resultat als auf vollständige Ausführung der Rechnung ankommt.

Mehrere Gleichungen mit mehreren Unbekannten.

Satz von Bézout.

35. Bézout hat zuerst bewiesen, dass die Elimination von $k-1$ Grössen zwischen k Gleichungen zu einer Endgleichung

führt, deren Grad höchstens gleich dem Producte der Grade der gegebenen Gleichungen ist.

Der Einfachheit wegen soll angenommen werden, dass vier vollständige und allgemeine Gleichungen gegeben seien mit den Unbekannten x, y, z und u und beziehungsweise vom Grade m, n, p und q, wo $m \geqq n \geqq p \geqq q$.

Aus der letzten Gleichung erhält man u^q unter ganzer Form durch die übrigen Unbekannten und die niedrigeren Potenzen von u ausgedrückt; dadurch können dann wieder die höheren Potenzen von u auf ähnliche Weise ausgedrückt werden; werden diese Ausdrücke in die anderen Gleichungen eingesetzt, so kommt u an keiner Stelle mit höherem Exponenten als $q-1$ vor. Aus der nächstletzten Gleichung wird darauf der Werth von z^p entwickelt, mit dem auf dieselbe Weise verfahren wird, und darauf entnimmt man y^n aus der zweiten Gleichung. Die erste Gleichung enthält nun kein Glied, welches theilbar wäre durch y^n, z^p oder u^q; dieselbe ist stets von ganzer Form, und die angewendeten Substitutionen haben der Homogenität, im früher angegebenen Sinne genommen, keinen Abbruch thun können.

Nun multiplicire man die erste Gleichung, welche nach y, z und u geordnet ist und x in den Coefficienten enthält, mit einem Polynom P, welches alle möglichen Glieder enthält, die nicht theilbar sind durch y^n, z^p oder u^q, und welches unbestimmte Coefficienten hat für alle Glieder mit Ausnahme des ersten, welches den Coefficienten 1 besitzt. Wenn die Multiplication ausgeführt ist werden wiederum wie vorhin die durch die Multiplication hinzugekommenen höheren Potenzen von y, z und u fortgeschafft; die Gleichung enthält nun ebenso viele Glieder mit y, z und u, wie unbestimmte Coefficienten vorhanden sind, und diese kommen linear in den Coefficienten der Gleichung vor; deshalb können sie so bestimmt werden, dass alle Glieder, welche y, z und u enthalten, fortfallen; man erhält dadurch eine Gleichung in x, welche die Endgleichung ist.

Um den Grad der Endgleichung zu bestimmen, beachte man, dass der Grad der ersten Gleichung m ist, während der

Factor, mit welchem multiplicirt wird, homogen von demselben Grade ist wie sein erstes Glied, wenn den Coefficienten passende Indices gegeben werden. Ist der Grad des Factors μ, so wird also das Product vom Grade $m + \mu$. Die Glieder, welche im Producte vorkommen, sind ihrer Anzahl nach npq, nämlich dieselben wie die, welche in dem Producte

$$(1 + y + \dots y^{n-1})(1 + z + \dots + z^{p-1})(1 + u + \dots + u^{q-1})$$

vorkommen, wenn jedes dieser Glieder mit einem gewissen Factor multiplicirt wird, der linear ist mit Rücksicht auf die unbestimmten Coefficienten. Eines der Glieder sei $l^{(r)}$ und dessen Coefficient in P sei $\alpha^{(r)}$; da $\alpha^{(r)}\, l^{(r)}$ vom Grade μ ist, so muss dieses Glied im Producte mit einem Factor multiplicirt sein, der eine Function von x und vom Grade m ist.

Das Product hat die Form

$$(a\,\alpha^{(0)} + b\,\alpha^{(1)} + \dots)\, l^{(0)} + (c\,\alpha^{(0)} + d\,\alpha^{(1)} + \dots)\, l^{(1)} \dots$$

Setzt man hier die Coefficienten von $l^{(0)}$, $l^{(1)} \dots$ gleich Null, und eliminirt darauf die Grössen $\alpha^{(0)}$, $\alpha^{(1)} \dots$, indem man auf gewöhnliche Weise eine Determinante bildet, so muss die Diagonalreihe in dieser von allen Coefficienten der Glieder von der Form $\alpha^{(r)}\, l^{(r)}$ gebildet werden; alle diese Coefficienten sind, wie gezeigt worden, von m^{ten} Grade, und ihr Product ist also vom Grade $mnpq$. Die Endgleichung ist also derartig beschaffen, dass die Summe der Indices in jedem ihrer Glieder $mnpq$ ist; wird x eingeführt, so erhält man deshalb eine Gleichung, welche höchstens vom Grade $mnpq$ ist. Dass der Grad nicht niedriger werden kann, wenn die Gleichungen allgemein sind, sieht man bei der Betrachtung der speciellen Gleichungen.

$$x = y^m;\; y = z^n;\; z = u^p;\; u = x^q.$$

36. Führt man einen unbestimmten Coefficienten weniger ein, so kann man alle Glieder fortschaffen mit Ausnahme desjenigen, welches eine Function von x allein ist, und desjenigen, welches eine der Unbekannten in der ersten Potenz zum Factor hat; man erhält dadurch die übrigen Unbekannten

durch Gleichungen ersten Grades bestimmt, sobald nur die eine Unbekannte aus der Endgleichung gefunden ist. Die weitere Untersuchung wird wie bei zwei Gleichungen, wenn man auf diese Euler's Methode anwendet, die im Wesentlichen dieselbe ist wie die von Bézout.

Beisp.

$$\begin{aligned} x^2 + yz &= a^2, \\ y^2 + xz &= b^2, \\ z^2 + xy &= c^2. \end{aligned}$$

Man erhält

$$\begin{aligned} y^2 &= b^2 - xz, \\ z^2 &= c^2 - xz, \\ y^2 z &= b^2 z - x c^2 + x^2 y, \\ y z^2 &= c^2 y - x b^2 + x^2 z, \\ y^2 z^2 &= b^2 c^2 - b^2 xy - c^2 xz + x^2 yz, \end{aligned}$$

und

$$(yz + \alpha_1 z + \beta_1 y + \gamma_2)(yz + x^2 - a^2) = 0.$$

Nach Ausführung der Multiplication und Einsetzung der Ausdrücke für y^2, z^2, $y^2 z$ und $y z^2$ erhält man, wenn die Coefficienten von $y z$, z und y sowohl wie das letzte Glied gleich Null gesetzt werden, und die Coefficienten, geschrieben in der angegebenen Ordnung, eliminirt werden, die Endgleichung

$$\begin{vmatrix} 2x^2 - a^2 & 0 & 0 & 1 \\ -c^2 x & 2x^2 - a^2 & b^2 & 0 \\ -b^2 x & c^2 & 2x^2 - a^2 & 0 \\ b^2 c^2 & -b^2 x & -c^2 x & x^2 - a^2 \end{vmatrix} = 0.$$

Man sieht, dass alle Glieder der einen Diagonalreihe vom zweiten Grade sind, in Uebereinstimmung mit dem, was über den Grad dieser Glieder im Allgemeinen bewiesen worden ist. Um y und z zu finden setze man

$$(z + \alpha_0 y + \alpha_1)(yz + x^2 - a^2) = 0,$$

also

$$z^2 y + \alpha_0 y^2 z + \alpha_1 yz + z(x^2 - a^2) + \alpha_0 y(x^2 - a^2) + \alpha_1 (x^2 - a^2) = 0,$$

woraus, wenn die Ausdrücke für $z^2 y$ und $y^2 z$ eingeführt und der Coefficient von yz gleich Null gesetzt wird:

$$z(2x^2 - a^2 + \alpha_0 b^2) + y[\alpha_0(2x^2 - a^2) + c^2] - x(b^2 + \alpha_0 c^2) = 0;$$

setzt man beziehungsweise die Coefficienten von z oder von y gleich Null, so wird

$$y[b^2 c^2 - (2x^2 - a^2)^2] = x[b^4 - c^2(2x^2 - a^2)];$$
$$z[b^2 c^2 - (2x^2 - a^2)^2] = x[c^4 - b^2(2x^2 - a^2)].$$

Die hier behandelten Gleichungen werden übrigens leichter aufgelöst, wenn man die beiden letzten addirt und multiplicirt und darauf $y + z$ und yz eliminirt. Die Endgleichung vom 8ten Grade wird auf den 4ten Grade reducirt, wenn man $x^2 = u$ setzt.

Poisson's Methode.

37. Vorläufig sollen drei Gleichungen von den Graden m, n und p betrachtet werden:

$$\varphi_m(x, y, z) = 0; \ \varphi_n(x, y, z) = 0; \ \varphi_p(x, y, z) = 0 \ \ldots\ldots \ (1).$$

Aus den beiden letzten wird z eliminirt; dadurch erhält man

$$z = \frac{\psi_1(x, y)}{\psi_2(x, y)}; \ \psi(x, y) = 0, \ \ldots\ldots\ldots\ldots \ (2)$$

wo die letzte Gleichung vom Grade np, und ψ_1 und ψ_2 ganze Functionen sind. Diese Gleichungen geben also, wenn x als bekannt betrachtet wird, np Werthe von y und zu jedem von diesen einen Werth von z. Die gegebenen Gleichungen werden als homogen, in der früher gebrauchten Bedeutung des Wortes, geschrieben, so dass z. B. der Coefficient von $y^r z^s$ in der ersten Gleichung den Index $m - r - s$ hat und eine ganze Function von x bedeutet, in welcher der höchste Exponent von x gleich dem Index ist. Die beiden durch die Elimination gebildeten Gleichungen sind dann homogen im gleichen Sinne. Symmetrische Functionen der np zusammengehörigen Wurzeln (y_1, z_1), $(y_2, z_2) \ldots$, d. h. solche, worin z_p mit z_q vertauscht wird, während gleichzeitig y_p mit

y_q vertauscht wird, werden symmetrische Functionen von $y_1, y_2 \ldots$, indem z mit Hülfe der ersten Gleichung fortgeschafft wird (2), und diese symmetrische Functionen können wieder mittelst der zweiten Gleichung (2) rational durch deren Coefficienten ausgedrückt werden, welche Functionen von x allein sind. Da alle Gleichungen, welche benutzt werden, homogen sind, müssen es auch die auf solche Weise gebildeten Gleichungen sein. Hat man z. B.

$$y_1 z_1 + y_2 z_2 + \cdots y_{np} z_{np},$$

so wird dieser Ausdruck erst umgeformt in

$$y_1 \frac{\psi_1(x, y_1)}{\psi_2(x, y_1)} + y_2 \frac{\psi_1(x, y_2)}{\psi_2(x, y_2)} + \cdots$$

und darauf durch x allein ausgedrückt, d. h. allein durch die mit Indices versehenen Coefficienten der gegebenen Gleichungen. Da die symmetrischen Functionen, welche hier behandelt werden, gebrochen sind, muss man erwarten, dass sie durch gebrochene Functionen von x ausgedrückt werden, bei denen der Unterschied zwischen dem Grade des Zählers und Nenners gleich dem Grade der symmetrischen Function ist. Indessen lässt sich beweisen, dass die gefundenen Functionen von x ganze Functionen werden, mit anderen Worten, dass der Nenner sich durch Division entfernen lassen muss. Im entgegengesetzten Fall müssten nämlich gewisse endliche Werthe von x existiren, für welche die ganze symmetrische Function von $y_1, z_1, y_2, z_2 \ldots$ unendlich würde, aber das kann nur stattfinden, wenn eine oder die andere der Grössen $y_1, z_1, y_2, z_2 \ldots$ unendlich ist. Die beiden Gleichungen $\psi_n = 0$ und $\psi_p = 0$ sind indessen vollständig allgemein, selbst wenn x einen besonderen Werth erhält, und von solchen Gleichungen weiss man, dass sie keine unendlichen Wurzeln haben können.

Die Bedingung dafür, dass der ersten Gleichung durch eines der gefundenen Werthsysteme genügt wird, ist nun

$$\varphi_m(x, y_1, z_1) \cdot \varphi_m(x, y_2, z_2) \cdots \varphi_m(x, y_{np}, z_{np}) = 0 \quad \ldots \ldots (3)$$

Dieses Product ist eine ganze symmetrische Function von $y_1, z_1, y_2, z_2 \ldots$ und kann also allein durch x ausgedrückt werden; die einzelnen Factoren sind homogen vom m^{ten} Grade, und der Grad wird dadurch nicht verändert, dass die symmetrischen Functionen fortgeschafft werden; also ist die Endgleichung in x vom Grade m n p.

38. Eliminirt man z aus den Gleichungen $\varphi_m = 0$ und $\varphi_n = 0$, so erhält man eine Gleichung in x und y vom Grade m n; eliminirt man z aus $\varphi_n = 0$ und $\varphi_p = 0$, so erhält man eine Gleichung vom Grade n p. Durch Elimination von y aus diesen beiden Gleichungen erhält man einerseits y rational ausgedrückt durch x, andrerseits eine Endgleichung vom Grade $m n^2 p$; *man kann also nicht auf diese Weise verfahren, ohne fremde Wurzeln einzuführen.* Dagegen kann man diese Elimination benutzen um y und dadurch wiederum z rational durch x auszudrücken.

Die Bedeutung der fremden Wurzeln lässt sich leicht erkennen. Von den beiden Gleichungen in x und y drückt die eine die Bedingungen dafür aus, dass φ_m und φ_n einen gemeinschaftlichen Factor haben, die andere dafür, dass φ_n und φ_p einen gemeinschaftlichen Factor haben. Die Endgleichung, welche auf diese Weise gebildet wird, drückt also die Bedingung dafür aus, dass eine gemeinschaftliche Wurzel in der ersten und zweiten Gleichung, und eine gemeinschaftliche Wurzel in der zweiten und dritten Gleichung existirt, während die Bedingung dafür gefunden werden sollte, dass alle drei Gleichungen eine gemeinschaftliche Wurzel haben. Sind die Wurzeln in den drei, mit Rücksicht auf z aufgelösten Gleichungen

$$z_1, z_2 \ldots z_m;\; z_1', z_2' \ldots z_n';\; z_1'', z_2'' \ldots z_p'',$$

müssen drei von ihnen, und zwar eine aus jeder Gruppe, gleich gross sein, und drei solche können auf m n p Arten entnommen werden, während man, wenn man eine der ersten Gruppe einer der zweiten Gruppe, und eine der zweiten Gruppe

einer der dritten Gruppe gleich setzt, dieses auf mn^2p verschiedene Arten thun kann.

Betrachtet man z. B. die drei Gleichungen, welche drei Flächen zweiter Ordnung angehören, so erhält man die Durchschnittscurven für die erste und zweite, und für die zweite und dritte Fläche auf die xy-Ebene als Curven vierter Ordnung projicirt, und diese Curven schneiden sich in 16 Punkten. 8 von diesen werden indessen nur Projectionen von Durchschnittspunkten der drei Flächen sein, während die übrigen 8 solche sind, deren z-Coordinaten wohl von den beiden Durchschnittscurven geschnitten werden, aber in zwei verschiedenen Punkten.

39. Es ist nun gezeigt worden, dass für drei Gleichungen vom Grade m, n und p im Allgemeinen die zwei Unbekannten rational durch die dritte ausgedrückt werden können, während diese durch eine Gleichung bestimmt wird, deren Grad höchstens mnp ist. Dass der Grad nicht niedriger werden kann, wenn die Gleichungen allgemein sind, ist früher gezeigt worden. In speciellen Fällen kann die Endgleichung von niedrigerem Grade werden, wenn nämlich eine oder mehrere der Wurzeln unendlich sind. Gleichfalls können die durch x rational ausgedrückten Werthe von y und z unbestimmt werden; das würde, wie bei zwei Gleichungen, andeuten, dass den betrachteten Werthen von x mehrere Werthe von y und z entsprechen, welche dann durch Gleichungen höherer Grade bestimmt werden.

Man sieht nun leicht, dass man die Geltung des bewiesenen Satzes auch auf vier Gleichungen mit vier Unbekannten u. s. w. ausdehnen kann. Darüber soll indessen hier ohne Aufenthalt hinweggegangen werden.

40. Die angegebene Methode zur Bestimmung symmetrischer Functionen simultaner Wurzeln ist sehr beschwerlich und kann auf folgende Weise vermieden werden. Man schreibe die erste Gleichung

$$a_m - u = 0,$$

worin a_m alle Glieder bezeichnet, welche x allein enthalten, u die übrigen Glieder; werden y_1, z_1, y_2, z_2 u. s. w. eingesetzt wie früher (37, (3)), so erhält u np Werthe $u_1, u_2 \ldots,$ und die Gleichung, welche gebildet werden soll, ist

$$(a_m - u_1)(a_m - u_2)(a_m - u_3)\ldots(a_m - u_{np}) = 0.$$

Nun wird z rational durch x und y ausgedrückt (37, (2)), und diese Ausdrücke werden in u eingesetzt, dann erhält man die Gleichung

$$u = \varphi(x.y);$$

wird y aus dieser und aus $\psi(x, y) = 0$ eliminirt, erhält man eine Gleichung in u vom Grade np; obgleich u eine gebrochene Function ist, sieht man doch durch dieselbe Betrachtung wie oben, dass die Coefficienten der Gleichung in u ganze Functionen von x sein müssen. Da die Gleichung in u folgendermassen geschrieben werden kann:

$$(u - u_1)(u - u_2)\ldots(u - u_{np}) = 0,$$

hat man nur nöthig in derselben a_m an die Stelle von u zu setzen, um die gesuchte Endgleichung zu erhalten.

Man könnte ebenso gut gleich a_m an die Stelle von u setzen und dadurch in Wirklichkeit y aus $\psi = 0$ und der ersten Gleichung, aus welcher z fortgeschafft ist, eliminiren; indessen würde dadurch die Form des Resultates geändert werden, so dass man den Factor, welcher fortdividirt werden soll, nicht gleich entdecken würde, während man, wenn man u behält, weiss, dass es der Coefficient von u^{np} ist, der durch Division entfernt werden kann.

Beisp. Aus

$$x^2 + yz = a^2,$$
$$y^2 + xz = b^2,$$
$$z^2 + xy = c^2,$$

erhält man

$$z = \frac{b^2 - y^2}{x}; \; y^4 - 2b^2 y^2 + x^3 y - c^2 x^2 + b^4 = 0;$$

$$yz = u = \frac{b^2 y - y^3}{x}; \; y^3 - b^2 y + u x = 0;$$

aus den beiden Gleichungen in y wird nun y eliminirt, der Coefficient von u^4 wird fortdividirt, und an Stelle von u wird $a^2 - x^2$ gesetzt; dadurch gelangt man zu der früher gefundenen Gleichung in x vom 8ten Grade.

Viertes Kapitel.

Transformation der Gleichungen.

Lineare Transformation.

41. Aus einer Gleichung können andere Gleichungen gebildet werden, deren Wurzeln in einem gewissen gegebenen Zusammenhang mit den Wurzeln der gegebenen Gleichung stehen. Ist die gegebene Gleichung

$$f(x) = 0, \quad \ldots \ldots \ldots \ldots \quad (1)$$

so wird häufig aus dieser eine Gleichung

$$\varphi(u) = 0 \quad \ldots \ldots \ldots \ldots \quad (2)$$

gebildet, wo zwischen einer Wurzel x der ersten und einer Wurzel u der zweiten Gleichung die Relation stattfindet

$$x = \frac{a + bu}{c + du}, \text{ oder } u = \frac{a - cx}{dx - b}, \quad \ldots \ldots \quad (3)$$

worin a, b, c und d gewisse von x und y unabhängige Grössen sind. Um die gesuchte Gleichung zu bilden, hat man nur in der gegebenen an Stelle von x den aus u dafür gebildeten Ausdruck zu setzen, wodurch man erhält

$$f\left(\frac{a + bu}{c + du}\right) = 0, \quad \ldots \ldots \ldots \ldots \quad (4)$$

welche Gleichung nach Fortschaffung der Brüche auf gewöhnliche Weise geordnet wird.

Da die Gleichung (1) dadurch aufgelöst werden kann, dass man zuerst die Gleichung $\varphi(u) = 0$ auflöst und darauf die gefundenen Werthe von u in den Ausdruck für x einsetzt, sieht man, dass beide Gleichungen von demselben Grade werden, und dass jeder Wurzel der einen eine Wurzel der andern entspricht, welche mit der ersteren in dem gegebenen Zusammenhange steht. Ist die eine Gleichung irreductibel, so ist die andere es auch, denn würde die eine Gleichung in einfachere Gleichungen zerlegt werden können, könnte man jede von diesen für sich transformiren und würde dadurch die gesuchte Gleichung aus mehreren andern zusammengesetzt erhalten. Man kann die Transformation dadurch vornehmen, dass man nach und nach

$$x = \frac{b}{d} + u_1;\ u_1 = \frac{ad - bc}{d^2 u_2};\ u_2 = \frac{c}{d} + u$$

setzt, so dass also alle unter die angeführte Form gehörigen Veränderungen auf folgende drei Formen zurückgeführt werden können

$$x = \alpha u;\ x = u + h;\ x = \frac{1}{u},$$

welche, jede für sich, genauer betrachtet werden sollen.

42. Durch Substitution von $x = \alpha u$ wird eine neue Gleichung gebildet, deren Wurzeln in einem gegebenen Verhältniss zu den Wurzeln der gegebenen Gleichung stehen. Falls die gegebene Gleichung gebrochene Coefficienten hat (für das Glied vom höchsten Grade wird der Coefficient 1 vorausgesetzt), kann α so gewählt werden, dass die Gleichung in u ganze Coefficienten bekommt; ist nämlich

$$f(x) = x^n + \frac{a_1}{b_1} x^{n-1} + \frac{a_2}{b_2} x^{n-2} \ldots + \frac{a_n}{b_n} = 0,$$

und setzt man $x = \frac{u}{\alpha}$, hat man nach Multiplication mit α^n,

$$\varphi(u) = u^n + \frac{a_1}{b_1} \alpha u^{n-1} + \frac{a_2}{b_2} \alpha^2 u^{n-2} \ldots + \frac{a_n}{b_n} \alpha^n = 0;$$

α wird nun so gewählt, dass alle Grössen

$$\frac{a_1 \alpha}{b_1}, \frac{a_2 \alpha^2}{b_2}, \ldots \frac{a_n \alpha^n}{b_n}$$

die Bruchform verlieren; dazu ist erforderlich, wenn alle ursprünglichen Brüche irreductibel sind, dass α alle Primfactoren oder verschiedenen Buchstabenfactoren enthält, welche in $b_1, b_2, \ldots b_n$ vorkommen. Um den Exponenten q zu finden, welchen ein in α vorkommender Factor β haben muss, beachte man, dass β^{pq} ein Factor von α^p werden wird; wenn man also im Nenner b_p den Factor β^ra ht, wird dieser fortdividirt werden können, sobald nur $pq \geqq r$ oder $q \geqq \frac{r}{p}$. Man dividirt deshalb die Exponenten der in den Nennern vorkommenden Factoren durch den Index des Gliedes und wählt zum Exponenten für β die kleinste ganze Zahl, welche gleich oder grösser ist als alle Exponenten, welche man auf diese Weise für β bekommen hat.

Beisp.

$$x^4 + \frac{1}{a b} x^3 + \frac{1}{a^2 b} x^2 + \frac{1}{a^4 b^2} x + \frac{1}{a^3 b^3} = 0.$$

Die Exponenten von a in den Nennern sind

$$1 \quad 2 \quad 4 \quad 3,$$

welche beziehungsweise durch 1, 2, 3 und 4 dividirt werden, wodurch man erhält

$$1 \quad 1 \quad \frac{4}{3} \quad \frac{3}{4}.$$

Die nächsthöhere ganze Zahl ist 2; für b erhält man

$$\begin{matrix} 1 & 1 & 2 & 3 \\ 1 & \frac{1}{2} & \frac{2}{3} & \frac{3}{4}, \end{matrix}$$

so dass man also

$$x = \frac{u}{a^2 b}$$

setzen muss. Die Gleichung wird dann

$$u^4 + a u^3 + a^2 b u^2 + a^2 b u + a^5 b = 0.$$

Nimmt man $\alpha = -1$ oder $x = -u$, so bildet man eine Gleichung, deren Wurzeln die der gegebenen mit entgegengesetztem Vorzeichen sind.

43. Bei der Substitution

$$x = u + h$$

kann man h derartig bestimmen, dass man eines der Glieder der Gleichung fortschafft. Man erhält nämlich durch Taylor's Formel, indem

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} \ldots + a_{n-1} x + a_n = 0, \quad \ldots (5)$$

$$f(h + u) = f(h) + f'(h) \frac{u}{1} + f''(h) \frac{u^2}{1.2} \ldots + \overset{(n-1)}{f}(h) \frac{u^{n-1}}{(n-1)!} + \overset{(n)}{f}(h) \frac{u^n}{n!}; \ (6)$$

der Coefficient von u^n ist 1, da $f^{(n)}(h) = n!$. Der Coefficient von u^{n-1} ist $a_1 + nh$; dies Glied wird also wegfallen, wenn

$$h = -\frac{a_1}{n}.$$

Der Coefficient von u^{n-2} ist

$$a_2 + (n-1) a_1 h + \tfrac{1}{2} n (n-1) h^2;$$

man kann also zwei Werthe für h wählen, welche dieses Glied zum Verschwinden bringen. Im Allgemeinen wird das Glied, welches u^{n-p} enthält, fortfallen für p Werthe von h, welche durch eine Gleichung vom p^{ten} Grade bestimmt werden. Soll das letzte Glied Null werden, wird h durch eine Gleichung vom n^{ten} Grade bestimmt, welche, mit Ausnahme der Bezeichnung für die Unbekannte, dieselbe ist wie die ursprüngliche. Da eine der Wurzeln Null ist, wenn das letzte Glied der Gleichung Null ist, so ist die Aufgabe, dieses Glied fortzuschaffen, auch dieselbe wie die, diejenigen Werthe von h zu finden, welche, von den Werthen von x subtrahirt, eine der Differenzen zu Null machen; das erfordert offenbar, dass h einer der Werthe von x sein muss.

Beisp.

$$x^3 + A x^2 + B x + C = 0$$

wird auf die Form

$$u^3 + a u + b = 0$$

gebracht, wenn man

$$x = u - \frac{A}{3}$$

nimmt; man erhält

$$a = B - \frac{A^2}{3}; \; b = C - \frac{1}{3} A B + \frac{2}{27} A^3.$$

44. Durch Combination der beiden erwähnten Substitutionen erhält man die Substitution

$$x = \alpha u + h;$$

hier soll der besondere Fall untersucht werden, wo

$$x = h - u \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (7)$$

Es kann sich ereignen, dass die Gleichung in u, abgesehen von der Bezeichnung der Unbekannten, mit der gegebenen Gleichung identisch wird; ist x_1 eine Wurzel dieser Gleichung, muss also $h - x_1$ auch eine Wurzel sein; nennt man diese Wurzel x_2, so wird also

$$x_1 + x_2 = h; \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (8)$$

da x_1 eine beliebige Wurzel ist, muss die gegebene Gleichung die Eigenschaft haben, dass je zwei ihrer Wurzeln zur Summe h haben; dies setzt jedoch voraus, dass die Gleichung von geradem Grade ist; ist sie von ungeradem Grade, muss die eine von den Wurzeln bei der Substitution unverändert bleiben; sie muss dann $\frac{1}{2} h$ sein, und der Factor $x - \frac{1}{2} h$ kann durch Division entfernt werden; es soll deshalb vorausgesetzt werden, dass die Gleichung von geradem Grade sei.

Eine solche Gleichung kann mit Hülfe einer Gleichung von halb so hohem Grade und mittelst quadratischer Gleichungen aufgelöst werden. Setzt man nämlich

$$y = x(h - x) \text{ oder } x^2 - h x + y = 0, \quad \ldots\ldots\ldots \quad (9)$$

und ist (5) die gegebene Gleichung, erhält y nur $\frac{n}{2}$ verschiedene Werthe, da die Werthe

$$y_1 = x_1(h - x_1) \text{ und } y_2 = x_2(h - x_2)$$

dieselben werden, weil $x_1 + x_2 = h$. Symmetrische Functionen der $\frac{n}{2}$ Werthe von y werden deshalb symmetrische Functionen der Wurzeln der gegebenen Gleichung; dadurch kann man die Gleichung in y bilden, aber dies geschieht leichter, wenn man x aus (9) und (5) eliminirt. Ist die Gleichung in y auflösbar, kann f(x) in $\frac{n}{2}$ Factoren vom zweiten Grade zerlegt werden, nämlich

$$f(x) = (x^2 - hx + y_1)(x^2 - hx + y_2) \dots (x^2 - hx + y_{\frac{n}{2}}).$$

Man sieht hieraus durch Vergleichung mit (5), dass

$$2a_1 = -nh$$

sein muss. Will man untersuchen, ob eine Gleichung von der Art der hier betrachteten ist, braucht man also nur zu untersuchen, ob die Gleichung unverändert bleibt, wenn man x mit $-\frac{2a_1}{n} - x$ vertauscht.

Beisp.

$$x^6 - 9x^5 + 30x^4 - 45x^3 + 25x^2 + 6x - 4 = 0.$$

Durch Vertauschung von x mit $3 - x$ bleibt die Gleichung unverändert; man eliminirt deshalb x mit Hülfe der Gleichung

$$x^2 - 3x + y = 0$$

und erhält

$$y^3 - 3y^2 - 2y + 4 = 0,$$

welche in

$$y - 1 = 0 \text{ und } y^2 - 2y - 4 = 0$$

zerfällt.

Reciproke Gleichungen.

45. **Durch die Substitution**

$$x = \frac{1}{u} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

wird eine Gleichung gebildet, deren Wurzeln die reciproken Werthe der Wurzeln der gegebenen sind. Gelangt man auf diese Weise zu einer Gleichung, welche identisch mit der gegebenen ist, so müssen je zwei ihrer Wurzeln zum Producte 1 haben, wenn die Gleichung von geradem Grade ist, während eine der Wurzeln ± 1 sein muss, wenn die Gleichung von ungeradem Grade ist. Im letzteren Falle soll angenommen werden, dass der Factor $x \mp 1$ durch Division entfernt sei; die Gleichung kann dann mit Hülfe einer Gleichung von halb so hohem Grade und mittelst quadratischer Gleichungen aufgelöst werden.

Setzt man nämlich

$$y = x + \frac{1}{x} \text{ oder } x^2 - xy + 1 = 0 \quad \ldots\ldots\ldots \quad (2)$$

so werden

$$y_1 = x_1 + \frac{1}{x_1} \text{ und } y_2 = x_2 + \frac{1}{x_2}$$

gleich gross sein, wenn $x_1 x_2 = 1$. y hat also nur halb so viele Werthe wie x. Die Gleichung in y wird gebildet durch Elimination von x aus der gegebenen Gleichung und (2).

Die Bedingung dafür, dass die gegebene Gleichung unter die hier betrachtete Art, die sogenannten reciproken Gleichungen, gehört, ist die, dass sie unverändert bleibt bei der Vertauschung von x mit $\frac{1}{x}$; dazu ist erforderlich, falls die Gleichung von geradem Grade ist, dass die Reihe der Coefficienten symmetrisch ist (der erste gleich dem letzten, der zweite gleich dem vorletzten u. s. w.); ist die Gleichung von ungeradem Grade, muss die Reihe der Coefficienten

symmetrisch sein, wenn man die Gleichung durch $x+1$ dividiren kann; kann man sie dagegen durch $x-1$ dividiren, muss die Reihe allerdings symmetrisch sein was den numerischen Werth der Coefficienten betrifft, aber die gleich grossen Coefficienten haben verschiedene Vorzeichen. Die allgemeine Form einer reciproken Gleichung von geradem Grade ist deshalb

$$x^{2n}+1+a_1\left(x^{2n-1}+x\right)+a_2\left(x^{2n-2}+x^2\right)+\ldots a_n x^n=0 \quad . \quad (3)$$

Die Reduction kann nun auf folgende Weise vorgenommen werden: Durch Division mit x^n erhält man

$$x^n+\frac{1}{x^n}+a_1\left(x^{n-1}+\frac{1}{x^{n-1}}\right)+a_2\left(x^{n-2}+\frac{1}{x^{n-2}}\right)\ldots+a_n=0 \quad . \quad (4)$$

Man setze nun

$$x+\frac{1}{x}=y, \quad \ldots\ldots\ldots\ldots \quad (5)$$

woraus

$$x^2+\frac{1}{x^2}=y^2-2$$

und, durch Multiplication dieser Gleichungen

$$x^3+\frac{1}{x^3}=y^3-3y.$$

Setzt man allgemein

$$x^p+\frac{1}{x^p}=s_p, \quad \ldots\ldots\ldots\ldots \quad (6)$$

erhält man durch Multiplication mit $x+\frac{1}{x}=y$

$$s_{p+1}=y\,s_p-s_{p-1}, \quad \ldots\ldots\ldots\ldots \quad (7)$$

welches zur successiven Berechnung von $s_3, s_4, s_5 \ldots$ dienen kann.

Eine allgemeine Formel für s_p erhält man mit Hülfe der Theorie der symmetrischen Functionen. x und $\frac{1}{x}$ sind nämlich Wurzeln der Gleichung

$$z^2-yz+1=0,$$

und es ist früher (24 (15)) gefunden worden:

$$s_p = y^p - p y^{p-2} + \frac{p(p-3)}{1.2} y^{p-4} \ldots$$

$$+ (-1)^\mu \frac{p(p-\mu-1)\ldots(p-2\mu+1)}{1.2.3\ldots\mu} y^{p-2\mu} \ldots \quad (8)$$

Wenn je zwei Wurzeln einer gegebenen Gleichung ein gewisses Product k haben, kann man durch die Substitution

$$x = u + \frac{k}{u}$$

die Gleichung ebenso wie die reciproken Gleichungen reduciren.

Beisp.

$$x^7 - 1 = 0.$$

Nach ausgeführter Division durch $x - 1$ erhält man

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0,$$

welche auf

$$u^3 + u^2 - 2u - 1 = 0$$

reducirt wird.

Aufgabe. Die Substitution

$$x = \frac{a + bu}{1 + u}$$

soll benutzt werden, um das zweite und dritte Glied der allgemeinen Gleichung dritten Grades fortzuschaffen.

Bildung von Gleichungen, in welchen eine Wurzel von mehreren Wurzeln einer gegebenen Gleichung abhängt.

46. Bisher ist jede Wurzel der gesuchten Gleichung als abhängig von einer der Wurzeln der gegebenen Gleichung

angenommen worden; man kann indessen auch Gleichungen bilden, in denen jede Wurzel auf eine gegebene Weise von mehreren Wurzeln der gegebenen Gleichung abhängt. Ein Beispiel dafür lieferte bereits die Gleichung der quadrirten Wurzeldifferenzen, in welcher jede Wurzel durch zwei Wurzeln der gegebenen Gleichung bestimmt ist. Allgemeiner kann man eine der Wurzeln der gesuchten Gleichung bestimmen durch

$$y = f(x_1, x_2 \dots x_p) \dots \dots \dots \dots (1)$$

Man erhält dann alle Wurzeln der gesuchten Gleichung, wenn man die unter dem Functionszeichen vorkommenden p Wurzeln auf alle möglichen Arten aus den Wurzeln der gegebenen Gleichung entnimmt; indem man f als rationale Function annimmt, wird dieselbe so viele Werthe bekommen, als es Möglichkeiten giebt, die p Wurzeln aus den Wurzeln der gegebenen Gleichung zu entnehmen. Werden alle Werthe durch $f_1, f_2 \dots f_\mu$ bezeichnet, so wird die gesuchte Gleichung

$$(y - f_1)(y - f_2) \dots (y - f_\mu) = 0 \dots \dots \dots \dots (2)$$

Da das Product auf der linken Seite eine symmetrische Function von $f_1, f_2 \dots f_\mu$ ist, wird es auch eine symmetrische Function der Wurzeln der gegebenen Gleichung und kann deshalb rational durch die Coefficienten dieser Gleichung ausgedrückt werden. Die gesuchte Gleichung hat deshalb rationale Coefficienten, wenn die gegebene solche hat, und ihr Grad wird durch die Anzahl der Werthe der Function bestimmt.

37. Man kann einen anderen Weg einschlagen und zu der gesuchten Gleichung durch Elimination gelangen, aber man wird bei dieser Methode fremde Wurzeln einführen, welche nachher fortgeschafft werden müssen. Als Beispiel soll die allgemeine Gleichung n^{ten} Grades genommen und die Gleichung gebildet werden, deren Wurzeln bestimmt werden durch

$$y = x_1 + \alpha x_2, \dots \dots \dots \dots (3)$$

worin α eine gegebene Grösse ist; man erhält dann

$$x_1 = y - \alpha x_2, \quad \ldots \ldots \ldots \ldots \quad (4)$$

und, da x_1 eine Wurzel der gegebenen Gleichung $f(x) = 0$ ist,

$$f(y - \alpha x_2) = 0. \quad \ldots \ldots \ldots \ldots \quad (5)$$

Ordnet man nun diese Gleichung nach x_2 und setzt x an Stelle von x_2, so müssen die beiden Gleichungen

$$f(y - \alpha x) = 0; \; f(x) = 0 \quad \ldots \ldots \ldots \ldots \quad (6)$$

eine Wurzel gemeinschaftlich haben; die Bedingung dafür erhält man durch Elimination von x; die Endgleichung ist dann die gesuchte Gleichung in y.

Man sieht indessen, dass die Gleichungen eine Wurzel gemeinschaftlich bekommen, wenn

$$y = x_p + \alpha x_q, \quad \ldots \ldots \ldots \ldots \quad (7)$$

aber das nicht nur, wenn p und q, wie die Aufgabe es fordert, verschieden sind, sondern auch, wenn sie gleich gross sind; die Endgleichung wird deshalb von fremden Wurzeln alle Werthe von

$$(1 + \alpha)\, x_p$$

bekommen.

Alle diese Grössen sind indessen Wurzeln der Gleichung

$$f\left(\frac{y}{1 + \alpha}\right) = 0 \quad \ldots \ldots \ldots \ldots \quad (8)$$

und können dadurch entfernt werden. Dadurch wird die Endgleichung, welche ursprünglich vom Grade n^2 ist, auf den Grad $n(n - 1)$ reducirt, übereinstimmend mit der Anzahl der Werthe von $x_1 + \alpha x_2$.

Für $\alpha = 1$ stimmen je zwei der Werthe überein; je zwei Wurzeln der Endgleichung werden gleich gross, und dieselbe kann durch Ausziehen einer Quadratwurzel auf den Grad $\frac{n(n-1)}{2}$ reducirt werden, welcher mit der Anzahl der Werthe von $x_1 + x_2$ übereinstimmt.

Später wird eine andere Methode angewendet werden, wodurch die hier gesuchte Gleichung durch Elimination gebildet wird ohne fremde Wurzeln einzuführen (vergl. Berechnung der imaginären Wurzeln in numerischen Gleichungen).

Auf ähnliche Weise sieht man, dass die Gleichung, deren Wurzeln Producte von je zwei Wurzeln der gegebenen Gleichung sind, durch Elimination von x aus

$$f(x) = 0 \text{ und } f\left(\frac{y}{x}\right) = 0 \quad \ldots\ldots\ldots\ldots \quad (9)$$

gebildet wird, wobei man von fremden Wurzeln die Quadrate der Wurzeln der gegebenen Gleichung erhält, während die Wurzeln, welche die Gleichung haben soll, jede zwei Male vorkommen.

48. Man kann zuweilen mit Vortheil die symmetrischen Relationen zwischen Wurzeln und Coefficienten benutzen um eine oder mehrere Wurzeln aus dem gegebenen Ausdruck fortzuschaffen und darauf die Elimination anwenden. Ist z. B. die gegebene Gleichung

$$x^3 + \alpha_1 x^2 + \alpha_2 x + \alpha_3 = 0$$

und

$$y_1 = \frac{x_1}{x_2 + x_3},$$

so benutze man die Relation

$$x_1 + x_2 + x_3 = -\alpha_1,$$

wodurch man erhält

$$y_1 = -\frac{x_1}{\alpha_1 + x_1},$$

so dass die gesuchte Gleichung erhalten wird durch Elimination von x aus der gegebenen Gleichung und

$$x(y + 1) + y\alpha_1 = 0.$$

Sollte man für dieselbe Gleichung die Gleichung der quadrirten Wurzeldifferenzen bilden, so wäre

$$y_1 = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1 x_2 = (\alpha_1 + x_3)^2 + \frac{4\alpha_3}{x_3},$$

und man müsste x aus der gegebenen Gleichung und

$$x y = x (\alpha_1 + x)^2 + 4 \alpha_3$$

eliminiren.

Methode von Tschirnhaus um Glieder aus einer Gleichung fortzuschaffen.

49. Die gegebene Gleichung sei

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} \ldots + a_{n-1} x + a_n = 0 \quad \ldots\ldots (1)$$

und es sei ferner

$$y = b_0 + b_1 x + b_2 x^2 + \ldots + b_p x^p, \quad \ldots\ldots\ldots (2)$$

wo $p < n$. Eliminirt man x aus (1) und (2), so gelangt man zu einer Gleichung in y, welche vom n^{ten} Grade wird, da y ebenso viele Werthe hat wie x. Um x zu eliminiren kann man eine der früher gezeigten Methoden benutzen oder auch die folgende: Man erhebt (2) auf die zweite, dritte u. s. w. Potenz, während man beständig mit Hülfe von (1) die Potenzen von x entfernt, die höher sind als x^{n-1}; man erhält dadurch eine Reihe Gleichungen von der Form

$$\left.\begin{array}{l} y^2 = c_0 + c_1 x + c_2 x^2 + \ldots \\ y^3 = d_0 + d_1 x + d_2 x^2 + \ldots \\ \ldots\ldots\ldots\ldots \end{array}\right\} \ldots\ldots\ldots\ldots (3)$$

In diese Gleichungen werden nach und nach für x alle Wurzeln der Gleichung (1) eingesetzt; man erhält dann durch Addition, wenn die Potenzsummen für (1) mit s, für (2) mit S bezeichnet werden:

$$\left.\begin{array}{l} S_1 = n b_0 + b_1 s_1 + b_2 s_2 + \ldots \\ S_2 = n c_0 + c_1 s_1 + c_2 s_2 + \ldots \\ S_3 = n d_0 + d_1 s_1 + d_2 s_2 + \ldots \end{array}\right\} \ldots\ldots\ldots\ldots (4)$$

Nun kann man $s_1, s_2 \ldots$ mit Hülfe bekannter Formeln berechnen und dadurch die Potenzsummen und wiederum dadurch die Coefficienten der Gleichung in y finden. Die

unbestimmten Coefficienten $b_0, b_1 \ldots b_p$ können darauf so bestimmt werden, dass so viele Coefficienten der neuen Gleichung, wie man will, Null werden; setzt man also

$$S_1 = 0,\ S_2 = 0,\ S_3 = 0,$$

wird das zweite, dritte und vierte Glied fortfallen; die erste Gleichung ist linear, die zweite vom zweiten, und die dritte vom dritten Grade mit Bezug auf die unbestimmten Coefficienten. Auf die Weise scheint es, dass man eine Gleichung sechsten Grades auflösen müsse, um diese drei Glieder fortzuschaffen; Jerrard hat indessen gezeigt, dass das zweite, dritte und vierte Glied aus einer jeden Gleichung mit Hülfe einer Gleichung dritten Grades fortgeschafft werden könne.

Die erste Gleichung $S_1 = 0$ ist linear und homogen mit Rücksicht auf $b_0, b_1 \ldots$; mit Hülfe dieser Gleichung kann man einen dieser Coefficienten aus den übrigen Gleichungen $S_2 = 0$ und $S_3 = 0$ fortschaffen, welche homogen vom beziehungsweise zweiten und dritten Grade sind und fortfahren es zu sein, nachdem der eine Coefficient fortgeschafft ist.

Nun wähle man $p = 4$, wodurch man über fünf Coefficienten zu disponiren hat. S_2 ist also eine homogene Function zweiten Grades von vier von diesen; eine solche Function kann immer auf die Form (vergl. 50)

$$\alpha_1 p_1^2 + \alpha_2 p_2^2 + \alpha_3 p_3^2 + \alpha_4 p_4^2$$

gebracht werden, worin α_1, α_2, α_3 und α_4 bekannte Grössen und p_1, p_2, p_3 und p_4 homogene lineare Functionen der unbestimmten Coefficienten sind; nun setze man

$$\alpha_1 p_1^2 + \alpha_2 p_2^2 = 0;\ \alpha_3 p_3^2 + \alpha_4 p_4^2 = 0, \quad \ldots\ldots \quad (5)$$

welche Gleichungen beide durch Ausziehen einer Quadratwurzel linear werden; mit Hülfe dieser werden darauf zwei der unbestimmten Coefficienten der Gleichung $S_3 = 0$ fortgeschafft, welche dann zur Bestimmung des Verhältnisses zwischen den beiden darin vorkommenden Coefficienten dient; der eine von diesen wird willkürlich gewählt, und die übrigen werden nun leicht gefunden, sobald die Gleichung dritten Grades gelöst ist.

50. Es wurde soeben der Satz benutzt, dass eine homogene Function zweiten Grades von mehreren Variablen auf eine gewisse besondere Form gebracht werden könne; dass dieses der Fall ist, lässt sich folgendermassen beweisen: $x_1, x_2 \ldots x_n$ seien die n Variablen; eine homogene Function zweiten Grades von diesen lässt sich dann darstellen in der Form

$$\alpha^2 x_1^2 + 2 \alpha P x_1 + Q,$$

worin α ein rationaler oder irrationaler Coefficient ist, und P und Q, welche beziehungsweise vom ersten und zweiten Grade sind, x_1 nicht enthalten; diese Grösse kann wieder auf die Form

$$(\alpha x_1 + P)^2 + Q - P^2$$

gebracht werden, worin $Q - P^2$ eine homogene Function zweiten Grades ist, welche x_1 nicht enthält, und welche nun auf ähnliche Weise behandelt werden kann; man erhält also auf diese Weise die Function dargestellt in Form einer Summe von quadratischen Gliedern, von welchen es höchstens so viele giebt, wie die Function Variable hat.

Durch Anwendung der entwickelten Methoden auf die allgemeine Gleichung fünften Grades oder deren reciproke Gleichung erhält man also eine der Formen

$$x^5 + ax + b = 0; \; x^5 + ax^4 + b = 0.$$

ZWEITER ABSCHNITT.

UEBER DIE ALGEBRAISCHE AUFLÖSUNG DER GLEICHUNGEN.

Erstes Kapitel.

Die Gleichung dritten Grades oder die cubische Gleichung.

Hudde's Methode.

51. Die cubische Gleichung

$$x^3 - 1 = 0 \quad \ldots\ldots\ldots\ldots \quad (1)$$

ist reductibel; die Wurzeln derselben sind 1, α und β, wenn

$$\alpha = \frac{-1 + i\sqrt{3}}{2};\ \beta = \frac{-1 - i\sqrt{3}}{2} \quad \ldots\ldots \quad (2)$$

Von Relationen zwischen diesen Wurzeln sind folgende bemerkenswerth:

$$1 + \alpha + \beta = 0;\ 1 + \alpha^2 + \beta^2 = 0;\ \alpha\beta = 1;$$
$$\alpha = \beta^2;\ \beta = \alpha^2.$$

Die allgemeine Gleichung dritten Grades oder die cubische Gleichung hat die Form

$$z^3 + Az^2 + Bz + C = 0,$$

welche indessen durch die Substitution

$$z = x - \frac{A}{3}$$

auf die Form

$$x^3 + ax + b = 0 \quad \ldots\ldots\ldots\ldots\ldots \quad (3)$$

gebracht werden kann.

Diese Gleichung lässt sich auf mehrfache Weise auflösen; zuerst soll Hudde's Methode betrachtet werden.

52. Für x werden zwei neue Unbekannte eingeführt, indem man

$$x = p + q \quad \ldots\ldots\ldots\ldots\ldots \quad (4)$$

setzt; dadurch wird die Gleichung

$$p^3 + q^3 + b + (3pq + a)(p + q) = 0.$$

Dieser Gleichung wird genügt, wenn p und q aus den beiden Gleichungen

$$p^3 + q^3 = -b; \; pq = -\frac{a}{3} \quad \ldots\ldots\ldots\ldots \quad (5)$$

bestimmt werden. Erhebt man die letztere auf die dritte Potenz, erhält man

$$p^3 q^3 = -\left(\frac{a}{3}\right)^3 \quad \ldots\ldots\ldots\ldots\ldots \quad (6)$$

Es wird darauf aufmerksam gemacht, dass diese Gleichung dieselbe geblieben wäre, wenn man a mit $a\alpha$ oder mit $a\beta$ vertauscht hätte.

Nun lassen sich p^3 und q^3 als Wurzeln der Gleichung

$$v^2 + bv - \left(\frac{a}{3}\right)^3 = 0 \quad \ldots\ldots\ldots\ldots \quad (7)$$

bestimmen, woraus

$$\left.\begin{matrix} p^3 \\ q^3 \end{matrix}\right\} = -\frac{b}{2} \pm \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}; \quad \ldots\ldots\ldots \quad (8)$$

daraus ergiebt sich

$$x = \sqrt[3]{-\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}} + \sqrt[3]{-\frac{b}{2} - \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}}, \quad \ldots\ldots \quad (9)$$

die sogenannte **cardanische** Formel.

Da die Cubikwurzel aus einer Zahl drei Werthe hat, erhält man neun Werthe für x; es sind sechs fremde Wurzeln dadurch eingeführt worden, dass (6) anstatt der zweiten Gleichung (5) benutzt worden ist; die neun Wurzeln gehören deshalb folgenden Gleichungen an:

$$\left.\begin{array}{l} x^3 + ax + b = 0, \\ x^3 + a\alpha x + b = 0, \\ x^3 + a\beta x + b = 0. \end{array}\right\} \quad \ldots \ldots \ldots \ldots \quad (10)$$

Um die Wurzeln dieser drei Gleichungen von einander zu trennen, ist zu beachten, dass für die drei Gleichungen beziehungsweise

$$pq = -\frac{a}{3};\; pq = -\frac{a\alpha}{3};\; pq = -\frac{a\beta}{3} \ldots \ldots \ldots \quad (11)$$

Sind also a und b reell, so müssen p und q so gewählt werden, dass ihr Product reell ist. Es sollen nun drei Fälle besonders betrachtet werden:

1. $\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3 > 0$. p^3 und q^3 sind reell, und p und q haben also jeder einen reellen Werth; werden diese reellen Werthe mit p_1 und q_1 bezeichnet, so werden alle Werthe

$$p_1,\; p_1\alpha,\; p_1\beta;\; q_1,\; q_1\alpha,\; q_1\beta.$$

Die gegebene Gleichung erhält deshalb die Wurzeln

$$x_1 = p_1 + q_1;\; x_2 = p_1\alpha + q_1\beta;\; x_3 = p_1\beta + q_1\alpha, \ldots \quad (12)$$

indem durch diese Bestimmung pq in allen drei Fällen reell wird. Dagegen werden die Wurzeln

$$\begin{array}{l} p_1 + q_1\alpha;\; p_1\alpha + q_1;\; p_1\beta + q_1\beta \\ p_1 + q_1\beta;\; p_1\beta + q_1;\; p_1\alpha + q_1\alpha \end{array}$$

beziehungsweise der zweiten und dritten der Gleichungen (10) angehören.

Man kann auch

$$x = p - \frac{a}{3p} \text{ oder } x = q - \frac{a}{3q} \ldots \ldots \ldots \quad (13)$$

setzen, und erhält dann nur die drei Wurzeln, welche wirklich der Gleichung angehören.

In dem hier untersuchten Falle hat die Gleichung eine reelle und zwei complexe Wurzeln.

2. Für $\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3 = 0$ werden p_1 und q_1 gleichgross. Die Gleichung hat dann drei reelle Wurzeln, aber von diesen sind zwei einander gleich.

3. $\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3 < 0$. In diesem Fall sind p^3 und q^3 complex. p und q sind dann auch complex, aber man kann immer zwei von ihren Werthen so wählen, dass $pq = -\frac{a}{3}$; bezeichnet man diese Werthe mit p_1 und q_1, so gelten die Formeln (12) auch hier. Dasselbe ist der Fall, wenn a und b imaginär sind.

Wenn a und b reell sind, erhalten alle Wurzeln complexe Form, aber es lässt sich zeigen, dass sie in diesem Falle dennoch alle reell sind. Es ist nämlich

$$p^3 = -\frac{b}{2} + i\sqrt{-\left(\frac{b}{2}\right)^2 - \left(\frac{a}{3}\right)^3};$$

$$q^3 = -\frac{b}{2} - i\sqrt{-\left(\frac{b}{2}\right)^2 - \left(\frac{a}{3}\right)^3} \quad \ldots\ldots\ldots \quad (14)$$

Setzt man nun

$$-\frac{b}{2} = r\cos\theta; \quad +\sqrt{-\left(\frac{b}{2}\right)^2 - \left(\frac{a}{3}\right)^3} = r\sin\theta, \quad \ldots \quad (15)$$

erhält man

$$p^3 = r(\cos\theta + i\sin\theta); \quad q^3 = r(\cos\theta - i\sin\theta), \quad \ldots \quad (16)$$

worin

$$r = \sqrt{-\left(\frac{a}{3}\right)^3}; \quad \cos\theta = \frac{-\frac{b}{2}}{\sqrt{-\left(\frac{a}{3}\right)^3}}; \quad \ldots\ldots \quad (17)$$

θ liegt im ersten oder zweiten Quadranten, da $\sin\theta$ positiv ist. Man erhält dann:

$$\left.\begin{aligned} p &= \sqrt{-\frac{a}{3}}\left(\cos\frac{2p\pi+\theta}{3} + i\sin\frac{2p\pi+\theta}{3}\right) \\ q &= \sqrt{-\frac{a}{3}}\left(\cos\frac{2p\pi+\theta}{3} - i\sin\frac{2p\pi+\theta}{3}\right) \end{aligned}\right\}, \quad \ldots (18)$$

also

$$x = 2\sqrt{-\frac{a}{3}}\cos\frac{2p\pi+\theta}{3}, \quad \ldots\ldots\ldots\ldots (19)$$

worin p die Werthe 0, 1 und 2 erhält.

Die drei Wurzeln sind also in diesem, dem sogenannten irreductiblen Fall, alle reell und ungleich gross; durch Wurzelgrössen können sie indessen nur unter imaginärer Form dargestellt werden. Jeder Versuch, p und q auf die Form

$$A \pm B\sqrt{-1}$$

ohne Anwendung trigonometrischer Functionen zu bringen, wird auf die gegebene Gleichung zurückführen.

Methode von Lagrange.

52. Lagrange sucht eine Function der Wurzeln zu bestimmen, um darauf, sobald diese bestimmt ist, die Wurzeln selbst zu finden. Die Function, welche Lagrange benutzt, ist

$$y = (x_1 + \alpha x_2 + \beta x_3)^3, \quad \ldots\ldots\ldots\ldots (1)$$

worin x_1, x_2 und x_3 die gesuchten Wurzeln sind, α und β die complexen Wurzeln der Einheit. Diese Function muss nämlich durch eine Gleichung zweiten Grades bestimmt werden, da sie nur zwei Werthe hat, denn je drei von den sechs Werthen, welche durch Vertauschung der Wurzeln

erhalten werden, müssen übereinstimmen; auf die Weise ist (51)

$$x_1 + \alpha x_2 + \beta x_3 = \alpha(\beta x_1 + x_2 + \alpha x_3) = \beta(\alpha x_1 + \beta x_2 + x_3),$$

also

$$(x_1 + \alpha x_2 + \beta x_3)^3 = (\beta x_1 + x_2 + \alpha x_3)^3 = (\alpha x_1 + \beta x_2 + x_3)^3.$$

y erhält deshalb nur zwei wirklich verschiedene Werthe, nämlich

$$y_1 = (x_1 + \alpha x_2 + \beta x_3)^3; \; y_2 = (\alpha x_1 + x_2 + \beta x_3)^3,$$

deren Summe und Product rational durch die Coefficienten der Gleichung ausgedrückt werden. Man erhält

$$y^2 + 27by - 27a^3 = 0.$$

Endlich werden die Wurzeln bestimmt durch

$$x_1 + x_2 + x_3 = 0;$$
$$x_1 + \alpha x_2 + \beta x_3 = \sqrt[3]{y_1};$$
$$\alpha x_1 + x_2 + \beta x_3 = \sqrt[3]{y_2}.$$

Die Discussion kann hier übergangen werden.

Methoden von Tschirnhaus und Euler.

54. Diese Methoden stimmen im Wesentlichen überein; indem man

$$y^2 + py + q = x \; \ldots\ldots\ldots\ldots\ldots \; (1)$$

setzt, werden p und q so zu bestimmen gesucht, dass man zu der gegebenen Gleichung gelangt, wenn man y aus (1) und

$$y^3 = d \; \ldots\ldots\ldots\ldots\ldots\ldots \; (2)$$

eliminirt. Die Form (2) kann man auch dadurch erhalten, dass man

$$x = \frac{p + qy}{1 + y}$$

setzt

Beisp.

$$x^3 + x^2 - 2x - 1 = 0,$$

$$x = y - \frac{1}{3};\ y^3 - \frac{7}{3}y - \frac{7}{27} = 0;\ \left(\frac{7}{54}\right)^2 - \left(\frac{7}{9}\right)^3 < 0.$$

$$\cos\theta = \frac{\frac{7}{54}}{\sqrt{\left(\frac{7}{9}\right)^3}} = \frac{1}{2\sqrt{7}};\ \theta = 79^0\,6'\,24'';$$

$$y = \frac{2}{3}\sqrt{7}\,.\cos\frac{2p\pi + \theta}{3}.$$

Aufgabe. In welcher irreductiblen cubischen Gleichung kann eine Wurzel als rationale Function einer andern Wurzel ausgedrückt werden?

Werden die beiden Wurzeln mit x_1 und x_2 bezeichnet, so kann man

$$x_1 = a + bx_2 + cx_2^2$$

setzen, da jede rationale Function einer Wurzel diese Form annehmen kan (26).

Nun sei die gesuchte Gleichung

$$f(x) = x^3 + px^2 + qx + r = 0,$$

und $\Psi(x) = 0$ möge die Gleichung darstellen, deren Wurzeln die drei Werthe von $a + bx_2 + cx_2^2$ sind. $f(x) = 0$ und $\Psi(x) = 0$ haben dann eine gemeinschaftliche Wurzel, und da $f(x) = 0$ irreductibel sein soll, müssen sie die übrigen Wurzeln auch gemeinschaftlich haben; da man nun z. B. nicht haben kann

$$x_3 = a + bx_3 + cx_3^2,$$

da x_3 in diesem Falle Wurzel einer Gleichung zweiten Grades werden würde, muss man haben

$$x_1 = a + bx_2 + cx_2^2,$$
$$x_2 = a + bx_3 + cx_3^2,$$
$$x_3 = a + bx_1 + cx_1^2.$$

Aus diesen Gleichungen ergibt sich

$$c = \frac{p^2 - 3q}{\sqrt{D}},\ \text{wo}\ D = (x_1 - x_2)^2 (x_2 - x_3)^2 (x_3 - x_1)^2 \quad \text{(vergl. 25).}$$

b und a erhalten $\sqrt{D}$ im Zähler, werden aber im Uebrigen rational durch die Coefficienten ausgedrückt. Die gesuchte Eigenschaft findet sich also bei allen cubischen Gleichungen, sobald $\sqrt{D}$ als bekannt vorausgesetzt werden darf. Je nachdem man $+\sqrt{D}$ oder $-\sqrt{D}$ nimmt, erhält man die eine oder die andere Wurzel durch die dritte ausgedrückt.

Zweites Kapitel.

Die Gleichung vierten Grades oder die biquadratische Gleichung.

Methode von Lagrange.

55. Wie man auch die allgemeine Gleichung vierten Grades auflösen möge, stets wird man genöthigt sein, eine Hülfsgleichung dritten Grades zu benutzen, die sogenannte *Resolvente;* die Unbekannte in dieser Gleichung ist eine solche Function der Wurzeln der gegebenen Gleichung, welche nur drei Werthe hat; solcher giebt es mehrere, z. B.

$$x_1 x_2 + x_3 x_4$$
$$(x_1 + x_2)(x_3 + x_4)$$
$$(x_1 - x_2 + x_3 - x_4)^2.$$

Lagrange benutzt die erste von diesen og setzt

$$y_1 = x_1 x_2 + x_3 x_4; \; y_2 = x_1 x_3 + x_2 x_4, \; y_3 = x_1 x_4 + x_2 x_3. \quad . \; . \; . \; (1)$$

Ist die gegebene Gleichung

$$f(x) = x^4 + A x^3 + B x^2 + C x + D = 0, \quad . \; . \; . \; . \; . \; . \; . \; (2)$$

so hat man

$$y_1 + y_2 + y_3 = B,$$
$$y_1 y_2 + y_1 y_3 + y_2 y_3 = \Sigma x_1^2 x_2 x_3 = AC - 4D,$$
$$y_1 y_2 y_3 = \Sigma x_1^3 x_2 x_3 x_4 + \Sigma x_1^2 x_2^2 x_3^2 = D(A^2 - 4B) + C^2.$$

Somit wird die Resolvente

$$y^3 - By^2 + (AC - 4D)y + D(4B - A^2) - C^2 = 0. \quad . \; . \; . \; (3)$$

Methode von Descartes.

56. Descartes setzte

$$f(x) = (x^2 + \alpha_1 x + \alpha_2)(x^2 + \beta_1 x + \beta_2),$$

woraus durch Vergleichung der Coefficienten

$$\begin{aligned} \alpha_1 + \beta_1 &= A \\ \alpha_1 \beta_1 + \alpha_2 + \beta_2 &= B \\ \alpha_1 \beta_2 + \beta_1 \alpha_2 &= C \\ \alpha_2 \beta_2 &= D. \end{aligned}$$

Nimmt man nun

$$\alpha_2 + \beta_2 = y$$

und eliminirt α_1, α_2, β_1 und β_2 aus den fünf Gleichungen, so gelangt man zu einer Gleichung in y, welche genau dieselbe ist, wie die oben gefundene. α_2 und β_2 sind nämlich die Producte von zwei Paar Wurzeln und folglich ist $\alpha_2 + \beta_2$ dieselbe Function der Wurzeln, welche Lagrange benutzt. Man könnte ebenso gut

$$y = \alpha_1 \beta_1 \text{ oder } y = (\alpha_1 - \beta_1)^2$$

setzen; dadurch würde y eine der übrigen Functionen mit drei Werthen, welche oben erwähnt wurden.

Ferrari's Methode.

57. Ferrari, der erste, welcher die Gleichung vierten Grades auflöste, gelangte zu derselben Resolvente wie Lagrange und Descartes. Er formt die Gleichung folgendermassen um

$$\left(x^2 + \frac{A}{2}x + \frac{y}{2}\right)^2$$
$$= \left(\frac{A^2}{4} - B + y\right)x^2 + \left(\frac{Ay}{2} - C\right)x + \frac{y^2}{4} - D, \quad \ldots \quad (1)$$

und sucht nun y so zu bestimmen, dass die rechte Seite ein Quadrat wird. Schreibt man die Bedingung hierfür hin, so erhält man eben die früher gefundene Resolvente. Man sieht auch leicht, dass y hier dieselbe Bedeutung hat, wie früher. Bezeichnet man nämlich den Werth, welchen die Grösse auf der rechten Seite erhält, sobald die Bedingung erfüllt ist, mit S^2, so erhält man

$$x^2 + \frac{A}{2}x + \frac{y}{2} \pm S = 0 \qquad (2)$$

Die Gleichung vierten Grades ist hierdurch in zwei Gleichungen zweiten Grades zerlegt worden, welche jede zwei der gesuchten Wurzeln geben; man hat also

$$x_1 x_2 = \frac{y}{2} + S; \quad x_3 x_4 = \frac{y}{2} - S,$$

also wie vorhin

$$y = x_1 x_2 + x_3 x_4.$$

Methoden von Tschirnhaus und Euler.

58. Tschirnhaus bringt die Gleichung auf die Form

$$y^4 + Py^2 + Q = 0,$$

indem er

$$y = a + bx + x^2$$

setzt und a und b so bestimmt, dass y^3 und y den Coefficienten 0 bekommen.

Euler eliminirt y aus

$$x = a + by + cy^2 + dy^3$$

und

$$y^4 = e,$$

und bestimmt a, b, c, d und e derartig, dass die gefundene Gleichung in x dieselbe wird, wie die gegebene. Die Unter-

suchung, wie die Unbekannte in der Gleichung dritten Grades, welche man auch bei diesen Methoden auflösen muss, von den Wurzeln abhängt, soll hier übergegangen werden. Euler hat sich auch einer Methode bedient, analog der von Hudde bei der Gleichung dritten Grades angewendeten, indem er

$$x = p + q + r$$

setzt. Man kann dann über diese neuen Unbekannten so disponiren, dass die gegebene Gleichung in drei Gleichungen zerlegt wird, durch welche $p^2 + q^2 + r^2$, $p^2 q^2 + p^2 r^2 + q^2 r^2$ und pqr bestimmt werden; p^2, q^2 und r^2 werden dann als Wurzeln einer Gleichung dritten Grades gefunden.

Genauere Untersuchung der Auflösung unter Anwendung der Methode von Descartes.

59. Für die Praxis wird die etwas veränderte Methode von Descartes vorzuziehen sein. Zuerst bringe man die Gleichung auf die Form

$$x^4 + ax^2 + bx + c = 0 \quad \ldots \ldots \ldots \ldots \quad (1)$$

und setze

$$x^4 + ax^2 + bx + c = (x^2 + \alpha x + \beta)(x^2 - \alpha x + \gamma), \quad \ldots \quad (2)$$

folglich

$$\left.\begin{array}{r} -\alpha^2 + \beta + \gamma = a, \\ \alpha(\gamma - \beta) = b, \\ \beta\gamma = c \end{array}\right\}; \quad \ldots \ldots \ldots \ldots \quad (3)$$

hieraus erhält man

$$\begin{aligned} \beta + \gamma &= a + \alpha^2, \\ \gamma - \beta &= \frac{b}{\alpha}, \\ 4\beta\gamma = 4c &= (a + \alpha^2)^2 - \frac{b^2}{\alpha^2}, \end{aligned}$$

oder

$$\alpha^6 + 2a\alpha^4 + (a^2 - 4c)\alpha^2 - b^2 = 0, \quad \ldots \ldots \ldots \quad (4)$$

welche Gleichung für $\alpha^2 = y$ reducirt wird auf

$$y^3 + 2ay^2 + (a^2 - 4c)y - b^2 = 0. \quad \dots\dots\dots \quad (5)$$

Die Gleichung in α hat sechs Wurzeln, nämlich die sechs Werthe von $x_1 + x_2$. Von diesen sind zwei und zwei gleich gross mit entgegengesetztem Vorzeichen, weil aus Gleichung (1) folgt

$$x_1 + x_2 + x_3 + x_4 = 0.$$

Sind a, b und c reell, so ist das letzte Glied der Resolvente negativ; sie hat dann immer eine positive Wurzel, während die beiden anderen beide positiv, beide negativ oder beide complex sind; $\alpha = \sqrt{y}$ wird deshalb immer reell für wenigstens einen Werth von y. Da nun

$$\beta = \frac{a + \alpha^2}{2} - \frac{b}{2\alpha}, \quad \dots\dots\dots\dots \quad (6)$$

so werden zwei Wurzeln bestimmt durch die Gleichung

$$x^2 + \alpha x + \frac{\alpha^3 + a\alpha - b}{2\alpha} = 0, \quad \dots\dots\dots \quad (7)$$

und die beiden anderen erhält man hieraus durch Vertauschung von α mit $-\alpha$.

Man sieht, dass die Wurzeln der gegebenen Gleichung durch Quadratwurzeln ausgedrückt werden können, falls die Resolvente eine rationale Wurzel hat. Später wird gezeigt werden, dass diese Bedingung nicht nur hinreichend, sondern auch nothwendig ist.

Ist

$$\frac{\alpha^2}{4} + \frac{a}{2} > \frac{b}{2\alpha},$$

sowohl für den negativen wie für den positiven Werth von α, so zeigt die quadratische Gleichung (7), dass *alle vier Wurzeln complex sind,* während sie *alle reell werden*, sobald die Grösse auf der linken Seite kleiner ist als jeder der Werthe von $\frac{b}{2\alpha}$; fällt sie zwischen diese beide Werthe, so sind *zwei Wurzeln reell* und *zwei complex.*

Hat die gegebene Gleichung *gleiche Wurzeln,* so müssen die beiden Gleichungen zweiten Grades entweder eine gemeinschaftliche Wurzel haben, oder eine von ihnen muss gleiche Wurzeln haben. Im letzteren Falle ist

$$\frac{\alpha^2}{4} + \frac{a}{2} = \pm \frac{b}{2\alpha}$$

oder

$$\left(\frac{\alpha^2}{4} + \frac{a}{2}\right)^2 = \frac{b^2}{4\alpha^2},$$

welche Gleichung, da $\alpha^2 = y$, auch geschrieben werden kann

$$y\left(\frac{y}{2} + a\right)^2 - b^2 = 0.$$

Da diese Gleichung eine Wurzel mit der Resolvente gemeinschaftlich haben soll, muss diese reductibel sein. Zu demselben Resultate gelangt man, wenn man annimmt, dass die beiden Gleichungen zweiten Grades eine Wurzel gemeinschaftlich haben.

60. Es ist gezeigt worden, dass man nur eine der Wurzeln der Resolvente zu benutzen braucht, um alle Wurzeln der gegebenen Gleichung auszudrücken. Man kann indessen auch alle Wurzeln der Resolvente benutzen. Bezeichnet man diese mit $\alpha_1{}^2$, $\alpha_2{}^2$, $\alpha_3{}^2$, so hat man nämlich

$$\alpha_1{}^2 + \alpha_2{}^2 + \alpha_3{}^2 = -2a;\ \alpha_1{}^2\,\alpha_2{}^2\,\alpha_3{}^2 = b^2 \text{ oder } \alpha_1\,\alpha_2\,\alpha_3 = b,$$

da man die Werthe von α_1, α_2 und α_3 so wählen kann, dass ihr Product dasselbe Vorzeichen hat wie b.

Dadurch erhält die Grösse, welche bei der Auflösung von

$$x^2 + \alpha x + \beta = 0$$

unter das Wurzelzeichen kommt, eine andere Form; man erhält

$$-\frac{\alpha^2}{4} - \frac{a}{2} + \frac{b}{2\alpha} = \frac{(\alpha_2 + \alpha_3)^2}{4},$$

und also

$$\left.\begin{matrix} x_1 \\ x_2 \end{matrix}\right\} = \frac{-\alpha_1 \pm (\alpha_2 + \alpha_3)}{2} \qquad (8)$$



und auf dieselbe Weise

$$\left.\begin{matrix} x_3 \\ x_4 \end{matrix}\right\} = \frac{\alpha_1 \pm (\alpha_2 - \alpha_3)}{2} \quad \ldots \ldots \ldots \ldots \ldots \quad (9)$$

Die Resolvente hat immer eine positive Wurzel; diese sei $\alpha_1{}^2$ und α_1 sei der positive Werth von $\sqrt{\alpha_1{}^2}$. $\alpha_2 \alpha_3$ muss dann dasselbe Vorzeichen haben wie b. Nun sind drei Fälle möglich:

1) $\alpha_2{}^2$ *und* $\alpha_3{}^2$ *sind beide positiv.* α_2 und α_3 müssen also mit gleichen Vorzeichen genommen werden, wenn b positiv ist, mit verschiedenen Vorzeichen, wenn b negativ ist. Die Wurzeln der gegebenen Gleichung *werden alle reell.*

2) $\alpha_2{}^2$ *und* $\alpha_3{}^2$ *sind beide negativ.* Man setze

$$\alpha_2{}^2 = -m; \; \alpha_3{}^2 = -n,$$

wo m und n positiv sind; dann erhält man

$$\alpha_2 = \mp i \sqrt{m}\,; \; \alpha_3 = \pm i \sqrt{n},$$

wenn b positiv ist, und

$$\alpha_2 = \pm i \sqrt{m}\,; \; \alpha_3 = \pm i \sqrt{n},$$

wenn b negativ ist. *Die Wurzeln der gegebenen Gleichung sind alle complex,* falls m und n ungleich gross sind. *Ist* $m = n$, *werden zwei Wurzeln gleich gross, die beiden anderen complex.*

3) $\alpha_2{}^2$ *und* $\alpha_3{}^2$ *sind beide complex;* dann setze man

$$\alpha_2{}^2 = r^2 (\cos\theta + i \sin\theta)\,; \; \alpha_3{}^2 = r^2 (\cos\theta - i \sin\theta)$$

also

$$\alpha_2 = \pm r \left(\cos\frac{\theta}{2} + i \sin\frac{\theta}{2}\right),$$

$$\alpha_3 = \pm r \left(\cos\frac{\theta}{2} - i \sin\frac{\theta}{2}\right),$$

worin die Vorzeichen von r gleich oder verschieden genommen werden müssen, je nachdem b positiv oder negativ ist; im ersten Falle hat man

$$\left.\begin{matrix} x_1 \\ x_2 \end{matrix}\right\} = \frac{-\alpha_1 \pm 2 r \cos\frac{\theta}{2}}{2},$$

$$\left.\begin{matrix} x_3 \\ x_4 \end{matrix}\right\} = \frac{\alpha_1 \pm 2 i r \sin\frac{\theta}{2}}{2};$$

im zweiten Falle erhält man

$$\left.\begin{matrix} x_1 \\ x_2 \end{matrix}\right\} = \frac{-\alpha_1 \pm 2ir \sin\frac{\theta}{2}}{2},$$

$$\left.\begin{matrix} x_3 \\ x_4 \end{matrix}\right\} = \frac{\alpha_1 \pm 2r \cos\frac{\theta}{2}}{2}.$$

Die gegebene Gleichung hat also *zwei reelle und zwei complexe Wurzeln.*

Drittes Kapitel.

Die binomische Gleichung.

Trigonometrische Ausdrücke für die Wurzeln.

61. Unter der binomischen Gleichung wird die Gleichung

$$z^n = a \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

verstanden. In dem Vorhergehenden sind bereits besondere hierunter mit einbegriffene Gleichungen vorgekommen; es soll jetzt die allgemeine Gleichung genauer untersucht werden.

Ist a complex, z. B.

$$a = a_1 + i b_1, \quad \ldots\ldots\ldots\ldots\ldots \quad (2)$$

so setze man

$$a_1 = r \cos \theta; \; b_1 = r \sin \theta \quad \ldots\ldots\ldots\ldots \quad (3)$$

und erhält dann

$$z = \sqrt[n]{r} \left(\cos \frac{2p\pi + \theta}{n} + i \sin \frac{2p\pi + \theta}{n} \right); \quad \ldots\ldots \quad (4)$$

hieraus erhält man die n gesuchten Werthe von z, wenn man p n auf einander folgende ganze Werthe beilegt. Die Wurzeln sind alle complex, denn um eine reelle Wurzel zu bekommen, müsste für einen ganzen Werth von p

$$\frac{2p\pi + \theta}{n} = k\pi$$

sein, wo k eine ganze Zahl bedeutet. Das ist indessen nur möglich für $\theta = 0$ oder $\theta = \pi$, was wiederum $b_1 = 0$ nach sich ziehen würde.

Ist a reell und k die positive Grösse, für welche

$$k^n = \pm a,$$

wird die Gleichung, wenn man

$$z = kx$$

setzt, auf

$$x^n = \pm 1$$

reducirt.

Man erhält nun wie oben aus

$$x^n = 1 \ldots\ldots (5)$$

$$x = \cos\frac{2p\pi}{n} + i\sin\frac{2p\pi}{n} \ldots\ldots (6)$$

und aus

$$x^n = -1 \ldots\ldots (7)$$

$$x = \cos\frac{(2p+1)\pi}{n} + i\sin\frac{(2p+1)\pi}{n} \ldots\ldots (8)$$

Im ersten Falle hat man eine reelle Wurzel, wenn $2p\pi = 0$ oder $2p\pi = n\pi$, indem p die Werthe $0, 1, 2 \ldots (n-1)$ erhält; ist nun n ungerade, so kann man nur $p = 0$ gebrauchen, und dem entspricht $x = 1$; ist n gerade, so kann man $p = 0$ und $p = \frac{1}{2}n$ nehmen, wodurch beziehungsweise $x = 1$ und $x = -1$. Die übrigen Wurzeln sind complex und paarweise conjugirt.

Im zweiten Falle erhält man reelle Wurzeln für

$$2p + 1 = 0 \text{ und } 2p + 1 = n;$$

die erste Bedingung kann nicht erfüllt werden und die zweite nur dann, wenn n ungerade ist; für ein gerades n erhält

man also lauter complexe Wurzeln, für ein ungerades n nur eine reelle Wurzel, nämlich $x = -1$. Die complexen Wurzeln sind auch hier paarweise conjugirt.

Eigenschaften der Wurzeln.

62. Ueber die Wurzeln dieser Gleichungen gelten verschiedene Sätze, welche oft Anwendung finden; es soll im Besonderen die Gleichung

$$x^n = 1$$

betrachtet werden.

Die gemeinschaftlichen Wurzeln für

$$x^n = 1 \text{ und } x^m = 1$$

werden durch die Gleichung

$$x^q = 1$$

bestimmt, worin q der grösste gemeinschaftliche Factor für m und n ist. Dies folgt daraus, dass $x^q - 1$ der grösste gemeinschaftliche Factor für $x^n - 1$ und $x^m - 1$ ist.

63. *Jede Potenz einer Wurzel der Gleichung*

$$x^n = 1$$

ist wieder eine Wurzel.

Denn ist α eine Wurzel, so ist $\alpha^n = 1$; α^p wird dann auch eine Wurzel sein, da $(\alpha^p)^n = (\alpha^n)^p = 1$.

64. *Wenn p eine Primzahl ist, können alle Wurzeln der Gleichung*

$$x^p = 1$$

dargestellt werden durch

$$\alpha, \alpha^2, \alpha^3 \ldots \alpha^p,$$

wo α eine willkürlich gewählte Wurzel ist, die Wurzel ausgenommen.

Da alle Grössen der Reihe Wurzeln sind, braucht man nur nachzuweisen, dass sie alle verschieden sind. Falls nun z. B.

$$\alpha^q = \alpha^r,$$

wo $q > r$, so müsste

$$\alpha^r (\alpha^{q-r} - 1) = 0$$

sein. Da α nicht Null ist, müsste also α eine Wurzel der Gleichung

$$x^{q-r} - 1 = 0$$

sein; das ist indessen unmöglich, denn da $q - r < p$, kann zufolge 62 diese Gleichung keine Wurzeln ausser 1 mit der gegebenen gemeinschaftlich haben. Ist p dagegen keine Primzahl, so können mehrere Glieder der Reihe gleich werden, so dass die Reihe nicht alle Wurzeln giebt. *Man nennt die Wurzeln primitiv, welche keine Gleichung von derselben Form aber von niedrigerem Grade befriedigen. Ist p eine Primzahl, sind alle Wurzeln primitiv mit Ausnahme von 1. Ist p keine Primzahl, wird die obenstehende Reihe dennoch alle Wurzeln geben, sobald α eine primitive Wurzel ist.* Ist p eine Potenz einer Primzahl, sind alle Wurzeln primitiv mit Ausnahme derjenigen, welche durch Gleichungen bestimmt werden, deren Exponenten niedrigere Potenzen derselben Primzahl sind. So sind i und $-i$ primitive Wurzeln für $p = 4$, während $+1$ und -1 nicht primitiv sind, da sie die Wurzeln der Gleichung $x^2 = 1$ darstellen. Alle Wurzeln können ausgedrückt werden durch α, α^2, α^3 und α^4, wenn $\alpha = i$ oder $\alpha = -i$, aber nicht wenn $\alpha = \mp 1$.

Dass eine Gleichung immer primitive Wurzeln hat, folgt aus dem Ausdruck für diese; sollten nämlich alle Wurzeln auch Wurzeln von Gleichungen von niedrigerem Grade sein, so müsste für jedes p

$$\frac{2p\pi}{n} = \frac{2p_1\pi}{n_1}$$

sein, wo $n_1 < n$. Das findet nur statt, wenn $\frac{p}{n}$ verkürzt

werden kann; *es giebt also so viele primitive Wurzeln, als es Zahlen giebt, kleiner als n, die prim zu n sind.* Diese Anzahl kann, wie bekannt, ausgedrückt werden durch

$$n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_q}\right),$$

wenn $p_1, p_2 \ldots p_q$ die Primfactoren von n sind.

65. *Sind m und n prim zu einander, und multiplicirt man alle Wurzeln von $x^m = 1$ mit allen Wurzeln von $x^n = 1$, so erhält man alle Wurzeln von $x^{mn} = 1$.*

Da nämlich eine Wurzel der ersten Gleichung das Argument $\frac{2p\pi}{m}$, eine der zweiten das Argument $\frac{2q\pi}{n}$ hat, so erhält das Product das Argument

$$\frac{2\pi(qm + pn)}{mn}$$

und ist folglich Wurzel der angegebenen Gleichung. Es bedarf nur noch des Nachweises, dass alle mn Werthe des Productes verschieden sind. Wären zwei Werthe gleich, müsste z. B.

$$qm + pn = q_1 m + p_1 n$$

sein, oder

$$\frac{m}{n} = \frac{p_1 - p}{q - q_1};$$

das ist indessen unmöglich, da $p_1 - p < m$, $q - q_1 < n$, und m und n prim zu einander sind.

Man sieht leicht, *dass die Geltung des Satzes auf eine beliebige Anzahl von Gleichungen, deren Exponenten prim zu einander sind, ausgedehnt werden kann. Gleichungen der angegebenen Form können dadurch auf Gleichungen zurückgeführt werden, deren Exponenten Potenzen von Primzahlen sind.*

66. *Die Gleichung*

$$x^{p^\mu} = 1,$$

wo p eine Primzahl bedeutet, lässt sich auf Gleichungen von der Form $x^p = a$ reduciren.

Die gegebene Gleichung kann nämlich durch folgendes System ersetzt werden:

$$x^p = \alpha_1;\ \alpha_1{}^p = \alpha_2;\ \alpha_2{}^p = \alpha_3;\ \ldots \alpha^p{}_{\mu-1} = 1.$$

Bei der Auflösung jeder dieser Gleichungen nehme man nur eine Wurzel, gleichgültig welche, doch 1 ausgenommen. Der Werth von x, zu dem man auf diese Weise gelangt, muss eine primitive Wurzel der gegebenen Gleichung sein, denn im entgegengesetzten Fall müsste er einer der Grössen $\alpha_1, \alpha_2, \alpha_3 \ldots$ den Werth 1 ertheilen, und für jede dieser Grössen ist eben ein Werth angenommen worden, der von 1 verschieden ist. Auf solche Weise ist also eine primitive Wurzel der gegebenen Gleichung gefunden, und aus dieser lassen sich alle übrigen Wurzeln durch Potenzirung bilden.

Auf diese Weise ist gezeigt worden, dass alle Gleichungen von der Form

$$x^n = 1$$

auf Gleichungen von der Form

$$x^p = \alpha$$

zurückgeführt werden können, wo p ein Primfactor von n, und α auf die oben angegebene Weise bestimmt ist.

67. Die symmetrischen Functionen der Wurzeln von $x^n - 1 = 0$ lassen sich leicht bestimmen; man hat nämlich

$$s_p = x_1{}^p + x_2{}^p \ldots + x_n{}^p = \alpha^p + \alpha^{2p} + \ldots + 1$$

oder

$$s_p = \frac{1 - \alpha^{np}}{1 - \alpha^p},$$

wenn α eine primitive Wurzel ist. Ist p nicht theilbar durch n, so ist der Zähler des Bruches Null, der Nenner nicht Null, also $s_p = 0$; ist p theilbar durch n, wird der Bruch unbestimmt, aber jedes Glied in s_p ist 1, also $s_p = n$. Hieraus folgt ferner

$$\Sigma\, x_1^\alpha x_2^\beta x_3^\gamma \ldots = 0$$

für alle Fälle, wo $\alpha + \beta + \gamma + \ldots$ nicht theilbar ist durch n; eine solche Function wird nämlich durch eine Summe von Gliedern von der Form

$$s_p \, s_q \, s_r \ldots$$

ausgedrückt, und ein solches Glied wird Null werden, sobald nicht alle Indices theilbar sind durch n; aber die Summe der Indices ist genau gleich der Summe der Exponenten der Function.

Anwendung der Theorie der reciproken Gleichungen auf die binomische Gleichung.

68. Die binomische Gleichung kann mit Hülfe der bei reciproken Gleichungen angewandten Methode auf eine Gleichung niedrigeren Grades reducirt werden.

Es soll nun die Gleichung

$$x^p = 1, \ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

wo p eine Primzahl ist, betrachtet werden; auf diese Form können, wie bekannt, die Fälle zurückgeführt werden, in denen p keine Primzahl ist. Sei $p = 2n + 1$, dann erhält man nach Division durch $x - 1$

$$x^{2n} + x^{2n-1} + x^{2n-2} \ldots + x + 1 = 0; \ldots\ldots\ldots \quad (2)$$

diese Gleichung ist reciprok und wird durch die Substitution

$$y = x + \frac{1}{x}$$

auf eine Gleichung in y vom n^{ten} Grade

$$U_n = 0 \ldots\ldots\ldots\ldots\ldots\ldots \quad (3)$$

reducirt. Diese Gleichung hat lauter reelle Wurzeln; man hat nämlich

$$x^2 - yx + 1 = 0, \ldots\ldots\ldots\ldots\ldots \quad (4)$$

woraus hervorgeht, dass einem Werthe von y zwei Werthe von x entsprechen, deren Summe y und deren Product 1; nun werden zwei solche Wurzeln ausgedrückt durch

$$x_1 = \cos\frac{2\,p_1\,\pi}{2n+1} + i\sin\frac{2\,p_1\,\pi}{2n+1};$$

$$x_2 = \cos\frac{2\,p_1\,\pi}{2n+1} - i\sin\frac{2\,p_1\,\pi}{2n+1},$$

so dass

$$y = 2\cos\frac{2\,p_1\,\pi}{2n+1} \quad \ldots\ldots\ldots\ldots\ldots \quad (5)$$

Die Wurzeln der Gleichung (3) sind also die n verschiedenen Werthe von $2\cos\frac{2\,p_1\,\pi}{2\,n+1}$, welche man erhält für $p_1 = 1, 2 \ldots n$. Da der in diesem Ausdruck vorkommende Bogen ein Vielfaches eines $(2n+1)^{\text{ten}}$ Theiles der Kreisperipherie ist und dieser Bogen durch Zirkel und Lineal bestimmt werden kann, sobald dessen Cosinus sich durch Quadratwurzeln ausdrücken lässt, so sieht man, dass die Aufgabe, eine Kreisperipherie mit Hülfe von Zirkel und Lineal in p gleich grosse Theile zu theilen zusammenfällt mit der, die Gleichung

$$x^p - 1 = 0$$

durch Quadratwurzeln aufzulösen. Für $p = 5$ wird die Gleichung in y quadratisch, so dass die Aufgabe lösbar ist; für $p = 7$ wird dagegen die Gleichung in y cubisch und kann nicht durch Quadratwurzeln aufgelöst werden. Später wird diese Aufgabe wieder aufgenommen werden. Hier soll nur noch folgender Satz bewiesen werden:

69. *Wenn p eine Primzahl ist, so ist die Gleichung*

$$\frac{x^p - 1}{x - 1} = 0$$

irreductibel.

X sei ein Polynom mit ganzen Coefficienten und lasse sich in zwei Factoren A und B von niedrigerem Grade zer-

legen. Dann müssen A und B mit ganzen Coefficienten dargestellt werden können. Enthalten nämlich A und B gebrochene Coefficienten, so kann man die Identität

$$X = AB$$

mit einer solchen Zahl k multipliciren, dass die Coefficienten die Bruchform verlieren; da nun kX durch einen Primfactor von k theilbar ist, muss auch einer von den Factoren auf der rechten Seite des Gleichheitszeichens dadurch theilbar sein*); deshalb kann man nach und nach alle Primfactoren von k auf beiden Seiten durch Division entfernen ohne Brüche einzuführen.

Nun nehme man an, dass

$$\frac{x^p - 1}{x - 1}$$

in zwei rationale Factoren zerlegt werden könne; diese müssen dann mit ganzen Coefficienten dargestellt werden können; vertauscht man auf beiden Seiten x mit $x + 1$, nimmt die linke Seite die Form

$$x^{p-1} + p\varphi(x) + p \quad \ldots\ldots\ldots\ldots \quad (6)$$

an, wo φ ein ganzes rationales Polynom ist. Die Glieder ohne x in den beiden Factoren müssen deshalb das Product p haben, und da p eine Primzahl ist, muss das eine ± 1, das andere $\pm p$ sein. Das Product hat deshalb die Form

$$(\pm 1 + a_1 x + a_2 x^2 + \ldots)(\pm p + b_1 x + b_2 x^2 \ldots).$$

Subtrahirt man auf beiden Seiten des Gleichheitszeichens

$$\pm p(\pm 1 + a_1 x + a_2 x^2 \ldots),$$

bleiben alle Glieder des Productes (6) mit Ausnahme von x^{p-1} theilbar durch p; daraus ersieht man, dass b_1 theilbar

*) Der Beweis, welcher im Allgemeinen für diesen Satz geführt wird, wenn A und B ganze Zahlen sind, gilt auch, wenn sie ganze Functionen sind; dass k in der Function aufgeht heisst dann, dass k in allen Coefficienten aufgeht.

sein muss durch p und so weiter. Zuletzt gelangt man auf diese Weise zu einer Gleichung von der Form

$$(\pm 1 + a_1 x + a_2 x^2 \ldots) x^\mu = x^{p-1} + p \varphi_1(x).$$

Hieraus würde folgen, dass p in dem Coefficienten von x^μ aufgehen müsse; das ist unmöglich, da der Coefficient ± 1 ist. Die untersuchte Gleichung ist also irreductibel.

Viertes Kapitel.

Die Gleichung fünften Grades.

Unmöglichkeit der algebraischen Auflösung dieser Gleichung.

70. Es ist gezeigt worden, dass die Auflösung der Gleichungen dritten und vierten Grades gelingt, weil es bei jeder dieser Gleichungen möglich ist Functionen der Wurzeln zu finden, welche eine geringere Anzahl von Werthen haben als die Wurzel selber, und welche deshalb durch Gleichungen von niedrigerem Grade als die gegebene bestimmt werden. Lagrange hat gezeigt, dass man, wenn man versucht die angewandten Methoden auf Gleichungen von höherem als dem vierten Grade auszudehnen, zu Hülfsgleichungen von höherem Grade als die gegebene gelangt. Hiernach war es wahrscheinlich, dass die Wurzeln einer Gleichung von höherem als dem vierten Grade im Allgemeinen nicht algebraisch durch die Coefficienten ausgedrückt werden könnten. Dass es sich wirklich so verhält hat Abel bewiesen; sein Beweis ist von Galois vereinfacht worden; der Beweis von Galois soll hier in etwas veränderter Form vorgeführt werden.

Falls eine Gleichung n^{ten} Grades mit allgemeinen Coefficienten durch Wurzelgrössen aufgelöst werden kann, muss dasselbe auch gelten von der Gleichung

$$x^n - (x_1 + x_2 \dots + x_n)\,x^{n-1} + (x_1 x_2 + x_1 x_3 + \dots)\,x^{n-2}$$
$$\dots \pm x_1 x_2 x_3 \dots x_n = 0, \quad \dots \quad (1)$$

worin $x_1, x_2 \ldots x_n$ vollkommen willkürlich und unabhängig von einander sind. Da die Wurzeln dieser Gleichung $x_1, x_2 \ldots x_n$ sind, muss die Auflösung zu diesen Werthen führen; alles Wurzelausziehen, welches bei der allgemeinen Auflösung verlangt wird, muss deshalb ausgeführt werden können, sobald man statt der allgemeinen Coefficienten $a_1, a_2 \ldots$ die Coefficienten der Gleichung (1) einsetzt.

Nun nehme man an, die erste Wurzel, welche ausgezogen werden solle, sei

$$y = \sqrt[r]{A}.$$

A enthält dann keine Wurzelgrössen, sondern ist eine rationale Function der Coefficienten der Gleichung und deshalb eine symmetrische Function von $x_1, x_2 \ldots x_n$. y kann dagegen keine symmetrische Function dieser Grössen sein, denn in solchem Falle könnte y rational durch die Coefficienten $a_1, a_2 \ldots$ der allgemeinen Gleichung ausgedrückt und die Wurzelgrösse durch einen rationalen Ausdruck ersetzt werden. Wenn y nicht symmetrisch ist, muss es wenigstens zwei von den darin vorkommenden Wurzeln, z. B. x_1 und x_2 geben, deren Vertauschung den Werth von y verändert. Da nun alle Werthe von y durch

$$y^r = A$$

bestimmt werden, muss der eine der beiden verschiedenen Werthe aus dem andern durch Multiplication mit einer der Wurzeln α (nicht 1) von $1^{\frac{1}{r}}$ gebildet werden. Man erhält dadurch, wenn $f(x_1, x_2 \ldots)$ der eine von den Werthen ist, welche durch Ausziehen der Wurzel erhalten werden,

$$f(x_1, x_2, x_3, x_4 \ldots x_n) = \alpha f(x_2, x_1, x_3, x_4 \ldots x_n).$$

Diese Gleichung muss eine Identität sein, da $x_1, x_2 \ldots$ unabhängig von einander sind; sie bleibt deshalb bestehen, wenn auf beiden Seiten des Gleichheitszeichens x_1 mit x_2 vertauscht wird; dadurch erhält man

$$f(x_2, x_1, x_3, x_4 \ldots x_n) = \alpha f(x_1, x_2, x_3, x_4 \ldots x_n).$$

Multiplicirt man diese Gleichung mit der vorhergehenden, erhält man

$$\alpha^2 = 1;\ \alpha = -1.$$

Man kann nun immer annehmen, dass r eine Primzahl ist, da man im entgegesetzten Fall mehrere Male nach einander mit einer Primzahl radiciren kann; dann muss $r = 2$ sein, da nur in diesem Falle $\alpha = -1$ sein kann. *Die erste Wurzel, welche auszuziehen ist, muss deshalb eine Quadratwurzel sein.* y ist eine rationale Function von $x_1, x_2 \ldots x_n$, welche das Vorzeichen wechselt, wenn x_1 und x_2 vertauscht werden und deshalb auch, wenn zwei beliebige Wurzeln vertauscht werden, da man vor der Ausziehung der Quadratwurzel A derartig ordnen kann, dass zwei beliebige Wurzeln an die Stellen kommen, welche früher von x_1 und x_2 eingenommen wurden.

y ist nicht symmetrisch, hat aber eine andere characteristische Eigenschaft; es muss nämlich unverändert bleiben bei jedem cyklischen Fortrücken von einer ungeraden Anzahl Wurzeln, z. B. wenn man x_1 statt x_2, x_2 statt x_3, x_3 statt x_1 setzt. Dies ist nämlich dasselbe, wie wenn man eine gerade Anzahl Vertauschungen von zwei Wurzeln vornimmt, und da y das Vorzeichen bei jeder solchen Vertauschung wechselt, muss es bei einer geraden Anzahl Vertauschungen unverändert bleiben.

Fährt man nun fort, indem man den gefundenen Ausdruck mit anderen ähnlichen und mit den symmetrischen Coefficienten combinirt, von neuem radicirt u. s. w., so giebt es zwei Möglichkeiten: entweder fahren die gefundenen Ausdrücke fort solche zu sein, welche nicht durch eine cyklische Vertauschung von 3 oder 5 Wurzeln verändert werden, oder man gelangt auch einmal dazu eine Wurzel auszuziehen, welche ein Resultat giebt, das diese Eigenschaft nicht hat; im ersteren Falle würde man zuletzt für einen der Werthe des gefundenen Ausdrucks erhalten

$$x_1 = f(x_1, x_2, x_3 \ldots x_n);$$

dies muss eine Identität sein, aber das ist unmöglich, sobald

mehr als zwei Wurzeln vorhanden sind, da die cyklische Verschiebung die linke, aber nach der Voraussetzung nicht die rechte Seite verändert.

Es ist also nothwendig, dass einmal eine Wurzelgrösse kommen muss, welche die erwähnte Eigenschaft des Ausdrucks nicht mehr besitzt; man muss also zu einem Ausdruck wie

$$z = \sqrt[r]{B}$$

gelangen, in welchem B durch cyklische Verschiebung unverändert bleibt, aber z nicht; man nehme an, dass z seinen Werth ändert, wenn x_1, x_2, x_3 beziehungsweise durch x_2, x_3, x_1 ersetzt werden. Die verschiedenen Werthe von z sind alle Wurzeln in

$$z^r = B;$$

man muss deshalb für die beiden Werthe von z eine Gleichung erhalten von der Form

$$f(x_1, x_2, x_3, x_4 \dots x_n) = \alpha f(x_2, x_3, x_1, x_4 \dots x_n).$$

Da diese Gleichung identisch ist, wird sie ihre Geltung behalten, wenn dieselben Vertauschungen auf beiden Seiten vorgenommen werden; dadurch erhält man

$$f(x_2, x_3, x_1, x_4 \dots x_n) = \alpha f(x_3, x_1, x_2, x_4 \dots x_n)$$

$$f(x_3, x_1, x_2, x_4 \dots x_n) = \alpha f(x_1, x_2, x_3, x_4 \dots x_n)$$

und durch Multiplication der drei Gleichungen

$$\alpha^3 = 1.$$

Es muss deshalb nothwendigerweise die Ausziehung einer Cubikwurzel vorkommen, sobald drei oder mehr Wurzeln vorhanden sind.

Die drei Werthe von z sollen mit

$$z, \ \alpha z, \ \alpha^2 z$$

bezeichnet werden. Giebt es nun mehr als vier Wurzeln, so kann man in der Identität

$$z^3 = B$$

eine cyklische Verschiebung von fünf Wurzeln vornehmen. B bleibt dadurch unverändert und z muss, da die Gleichung ihre Geltung behält, entweder unverändert bleiben oder in αz oder $\alpha^2 z$ übergehen; im letzten Falle kann man wie früher verfahren und erhält dadurch

$$\alpha^5 = \pm 1;$$

das ist unmöglich, da α einer der complexen Werthe von $1^{\frac{1}{3}}$ ist.

Es bleibt also nur die Möglichkeit übrig, dass z unverändert bleiben kann bei jeder cyklischen Verschiebung von fünf Wurzeln, während es bei der cyklischen Verschiebung von drei Wurzeln mit α oder α^2 multiplicirt wird.

Eine cyklische Verschiebung von drei Grössen kann indessen ersetzt werden durch zwei cyklische Verschiebungen von fünf Grössen; so wird die cyklische Verschiebung von

$$x_1,\ x_3,\ x_2$$

dadurch ausgeführt werden können, dass man erst

$$x_5,\ x_4,\ x_3,\ x_1,\ x_2$$

und darauf

$$x_1,\ x_2,\ x_3,\ x_4,\ x_5$$

verschiebt, wodurch zwei cyklische Verschiebungen von fünf Wurzeln vorgenommen worden sind. Da nun keine von diesen z verändert, wird z durch eine cyklische Verschiebuug von drei Wurzeln unverändert bleiben, aber das widerstreitet der Voraussetzung. Es ist also bewiesen, dass *allgemeine Gleichungen von höherem als dem vierten Grade nicht algebraisch*) aufgelöst werden können.*

---

*) „Algebraisch“ ist hier als „durch Wurzelausziehen und andere algebraischen Operationen zu verstehen. Abel und Galois betrachten auch die Möglichkeit, dass man für x_1 einen algebraischen Ausdruck finden könnte, der sich nicht identisch auf x_1 reduciren liesse.

Fünftes Kapitel.

Zerlegung rationaler Polynome in rationale Factoren.

Factoren ersten Grades.

71. Die möglicherweise vorhandenen Factoren ersten Grades eines rationalen Polynoms $f(x)$ kann man immer finden. Ein solcher Factor muss nämlich von der Form $x - \alpha$ sein, und α muss dann ein Factor des Gliedes von $f(x)$ sein, welches x nicht enthält; später wird diese Aufgabe wieder aufgenommen werden; hier soll nur bemerkt werden, dass man den Versuch mit allen Factoren machen kann, welche sich in dem letzten Gliede finden; genügt keiner von diesen der Gleichung $f(x) = 0$, so hat dieselbe keine rationale Wurzel und $f(x)$ keinen rationalen Factor ersten Grades.

Allgemeiner Ausdruck für einen Factor von f(x).

72. Die gegebene Gleichung vom n^{ten} Grade und ohne gleiche Wurzeln sei

$$f(x) = 0 \quad \dots\dots\dots\dots\dots\dots \quad (1)$$

mit den Wurzeln

$$x_1, x_2, x_3, \dots x_n;$$

ferner sei

$$y_1 = \varphi_1(x_1, x_2, \ldots x_p), \quad \ldots \ldots \ldots \ldots \quad (2)$$

wo φ eine gewisse ganze rationale Function der p Wurzeln bedeutet. Nun seien

$$\varphi_1, \varphi_2 \cdots \varphi_r$$

alle die algebraisch *verschiedenen* Ausdrücke, welche aus φ dadurch gebildet werden können, dass man die darin vorkommenden Wurzeln auf alle möglichen Arten aus den Wurzeln der Gleichung entnimmt, während

$$y_1, y_2 \cdots y_q$$

die numerischen Werthe (Zahlenwerthe) derjenigen von diesen bezeichnen mögen, in welchen eine der Wurzeln, z. B. x_1, auf ihrem ursprünglichen Platze geblieben ist. Die Werthe von φ werden durch eine Gleichung mit rationalen Coefficienten bestimmt; nun nehme man an, dass y_1 eine α fache Wurzel dieser Gleichung sei, so dass

$$y_1 = \varphi_1 = \varphi_2 = \varphi_3 \cdots = \varphi_\alpha.$$

Jetzt bilde man die Gleichuug

$$(y - y_1)(y - y_2) \cdots (y - y_q) = 0. \quad \ldots \ldots \ldots \quad (3)$$

Die Coefficienten dieser Gleichung sind symmetrische Functionen der Wurzeln der Gleichung

$$\frac{f(x)}{x - x_1} = 0,$$

und können deshalb rational durch x_1 und bekannte Grössen ausgedrückt werden; dadurch wird (3) auf die Form

$$F(y, x_1) = 0 \quad \ldots \ldots \ldots \ldots \quad (4)$$

gebracht.

Da y_1 eine Wurzel dieser Gleichung ist, hat man identisch

$$F(y_1, x_1) = 0, \quad \ldots \ldots \ldots \ldots \quad (5)$$

aber hierdurch wird zugleich ausgedrückt, dass x_1 eine Wurzel der Gleichung

$$F(y_1, x) = 0 \quad \ldots \ldots \ldots \ldots \quad (6)$$

ist, mithin eine gemeinschaftliche Wurzel für diese Gleichung und die gegebene.

Es soll nun untersucht werden, ob diese Gleichungen irgend welche andere gemeinschaftliche Wurzeln, z. B. x_m, haben können. Die Bedingung hierfür ist

$$F(y_1, x_m) = 0,$$

und dieser Gleichung wird genügt, sobald y_1 eine Wurzel ist von

$$F(y, x_m) = 0.$$

Diese Gleichung wird aus (4) durch Vertauschung von x_1 und x_m gebildet, und kann deshalb auch aus der mit (4) identischen Gleichung (3) auf dieselbe Weise gebildet werden; bei dieser Vertauschung gehen $y_1, y_2 \ldots$ in Werthe von φ über, so dass die Bedingung dafür, dass x_m eine gemeinschaftliche Wurzel ist, darin besteht, dass es einen Werth φ_κ von φ giebt, in welchem x_m an der Stelle von x_1 steht, und für welchen

$$y_1 = \varphi_k.$$

Die letzte Bedingung wird erfüllt für

$$k = 1, k = 2, \ldots k = \alpha.$$

Die beiden Gleichungen

$$f(x) = 0 \text{ und } F(y_1, x) = 0 \quad \ldots \ldots \ldots \ldots \quad (7)$$

haben also alle Wurzeln gemeinschaftlich, welche in

$$\varphi_1, \varphi_2, \ldots \varphi_\alpha \quad \ldots \ldots \ldots \ldots \quad (8)$$

den Platz von x_1 einnehmen können.

Aus diesem Satze, der in etwas abweichender Form von Lagrange und Galois gegeben worden ist, lassen sich mehrere wichtige Schlussfolgerungen ziehen, wie nun gezeigt werden soll.

73. *Falls die Gleichung in φ keine gleichen Wurzeln hat,* hat man nur

$$y_1 = \varphi_1;$$

ist nun φ derartig unsymmetrisch, dass *keine andere Wurzel den Platz von x_1 einnehmen kann, ohne dass φ sich algebraisch verändert*, so bleibt x_1 die einzige Wurzel, welche den beiden Gleichungen gemeinschaftlich ist, und *kann deshalb rational durch y_1 und bekannte Grössen ausgedrückt werden.* Im Besonderen gilt dieser Satz für alle Wurzeln der Gleichung, sobald man den Werth einer solchen Function

$$y = \varphi(x_1, x_2 \ldots x_n)$$

kennt, welche lauter verschiedene Werthe für alle möglichen $n!$ Vertauschungen der Wurzeln bekommt. In dieser speciellen Form hat Galois den Satz bewiesen.

Sobald φ_1 entweder ganz oder theilweise symmetrisch ist, würden alle die Wurzeln, welche den Platz von x_1 einnehmen können, ohne dass der Ausdruck algebraisch verändert wird, Wurzeln der Hülfsgleichung und folglich gemeinschaftlich für beide Gleichungen werden. Im Besonderen beachte man den Fall, wo alle Wurzeln in φ_1 vertauscht werden können; die beiden Gleichungen erhalten dann die p Wurzeln gemeinschaftlich, und dadurch dass man den grössten gemeinschaftlichen Factor sucht, *kann man die Gleichung bilden, welche diese Wurzeln bestimmt oder den diesen Wurzeln entsprechenden Factor p^{ten} Grades von $f(x)$.* Die allgemeine Form für einen Factor p^{ten} Grades von $f(x)$ ist deshalb

$$x^p + \varphi_1(y_1)\, x^{p-1} + \varphi_2(y_1)\, x^{p-2} \ldots + \varphi_p(y_1), \quad \ldots\ldots (9)$$

worin $\varphi_1, \varphi_2 \ldots \varphi_p$ rationale Functionen sind von bekannten Grössen und von y_1, welches der Werth einer solchen symmetrischen Function der p Wurzeln ist, deren Bestimmungsgleichung lauter ungleich grosse Wurzeln hat. Man kann also in diesem Falle alle symmetrischen Functionen der p Wurzeln als rationale Functionen einer derselben und bekannter Grössen ausdrücken.

Beisp. 1. Für die Gleichung

$$x^3 - 6x^2 + 11x - 6 = 0$$

ist gegeben

$$x_1^2 + x_2^2 = 5;$$

man setze

$$y_1 = x_1^2 + x_2^2;\ y_2 = x_1^2 + x_3^2$$

und erhält, wenn man x_2 und x_3 fortschafft,

$$y^2 - (x_1^2 + 14)\,y + 14\,x_1^2 + \frac{36}{x_1^2} = 0$$

oder, wenn man x statt x_1 und 5 statt y einsetzt,

$$x^4 - 5x^2 + 4 = 0,$$

welche Gleichung mit der gegebenen die beiden Wurzeln gemeinsam hat, welche durch

$$x^2 - 3x + 2 = 0$$

bestimmt werden.

Beisp. 2. Die allgemeine Form für einen Factor zweiten Grades von

$$f(x) = x^3 + ax^2 + bx + c$$

soll ausgedrückt werden durch das Product y von zwei Wurzeln von $f(x) = 0$.

$$y_1 = x_1 x_2;\ y_2 = x_1 x_3;$$

$$x_2 + x_3 = -a - x_1,$$

also

$$y^2 + (x_1^2 + a x_1)\,y - x_1 c = 0,$$

woraus die gesuchte Form

$$x^2 + \frac{ay - c}{y}\,x + y.$$

74. Die Gleichung in φ, welche oben benutzt wurde, gehört in dem Falle, wo sie $n!$ verschiedene Wurzeln hat, einer besonderen Klasse von Gleichungen an, welche sogleich

genauer untersucht werden soll; sie hat nämlich die Eigenschaft, dass *jede ihrer Wurzeln rational durch jede der übrigen Wurzeln ausgedrückt werden kann.* Jede der Wurzeln ist nämlich eine rationale Function von $x_1, x_2 \ldots x_n$, und jede von diesen kann wieder rational durch einen beliebigen Werth von φ ausgedrückt werden.

Man kann dieses benutzen, *um so viele algebraisch irrationale Grössen, wie man will, rational durch eine irrationale Grösse auszudrücken, unter einer algebraisch irrationalen Grösse jede Wurzel einer Gleichung mit rationalen Coefficienten verstanden, einerlei ob diese Wurzel sich algebraisch ausdrücken lässt oder nicht;* sind nämlich $x_1, x_2 \ldots x_p$ die irrationalen Grössen, welche als Wurzeln derselben oder verschiedener algebraischer Gleichungen bestimmt sind, so kann man immer eine neue algebraische Gleichung mit rationalen Coefficienten bilden (z. B. durch Multiplication aller gegebenen Gleichungen mit einander), unter deren Wurzeln sich $x_1, x_2 \ldots x_p$ finden; bildet man nun aus den Wurzeln dieser Gleichung eine solche Function, welche für alle Vertauschungen der Wurzeln verschiedene Werthe hat, so werden sich alle Wurzeln der Gleichung und also auch die gegebenen irrationalen Grössen rational durch diese ausdrücken lassen. Einer solchen Function kann man z. B. die Form

$$y = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 \ldots + \alpha_n x_n \ldots \ldots \ldots \quad (10)$$

geben, wenn man annimmt dass die Hülfsgleichung vom n^{ten} Grade ist. Es ist einleuchtend, dass die Coefficienten $\alpha_1, \alpha_2 \ldots \alpha_n$, da $x_1, x_2 \ldots$ verschieden sind, immer so gewählt werden können, dass alle Werthe der Function verschieden werden.

75. Wie oben werde vorausgesetzt, dass die gegebene Gleichung vom n^{ten} Grade sei, und dass φ $n!$ verschiedene Werthe habe; es ist indessen möglich, dass die Gleichung in φ reductibel sei; in diesem Falle nehme man an, dass sie in lauter irreductible Gleichungen zerlegt sei, und dass eine von diesen die Wurzeln

$$\varphi_1, \varphi_2 \ldots \varphi_p \ldots \ldots \ldots \ldots \quad (11)$$

habe.

Man kann dann, wie gezeigt worden, jede Wurzel der gegebenen Gleichung als eine rationale Function eines dieser Werthe von φ ausdrücken, so dass man z. B. für die Wurzeln erhalten würde:

$$\Psi_1(\varphi_1), \Psi_2(\varphi_1) \ldots \Psi_n(\varphi_1) \ldots\ldots\ldots\ldots (12)$$

Wenn man in dieser Reihe φ_1 mit einer beliebigen von den Grössen (11) vertauscht, wird sie dennoch fortfahren alle Wurzeln der gegebenen Gleichung, nur in veränderten Reihenfolge, zu geben.

Um eine der Wurzeln, z. B. x_1 zu finden, setze man nämlich

$$y_1 = \varphi_1;$$

aus φ_1 kann man nun eine andere von den Grössen der Reihe (11) bilden, indem man die Wurzeln in φ_1 auf eine gewisse Weise vertauscht; das Verfahren der Rechnung bleibt nun in beiden Fällen dasselbe, wenn nur diese Vertauschung der Wurzeln überall stattfindet; fand man früher

$$x_1 = \Psi_1(\varphi_1),$$

so findet man nun also

$$x_p = \Psi_1(\varphi_p),$$

wo x_p die Wurzel ist, welche an die Stelle von x_1 kommt, wenn φ_1 mit φ_p vertauscht wird. Die neuen Werthe sind alle verschieden, denn wenn z. B. $\Psi_1(\varphi_p) = \Psi_2(\varphi_p)$, würde φ_p eine gemeinschaftliche Wurzel der Gleichung $\Psi_1(\varphi) - \Psi_2(\varphi) = 0$ und der irreductiblen Gleichung mit den Wurzeln (11) sein. Man müsste dann auch haben $\Psi_1(\varphi_1) - \Psi_2(\varphi_1) = 0$ (13), aber alle Grössen (12) sind verschieden.

Dieser Satz ist es, welcher der Anwendung der Substitutionstheorie in der Theorie der Gleichungen zu Grunde liegt, wie später gezeigt werden wird.

76. Aus der voranstehenden Entwicklung folgt, dass es, falls f(x) rationale Factoren hat, immer möglich ist, dieselben

zu finden; ist z. B. ein rationaler Factor vom p^{ten} Grade vorhanden, so muss es unter den Wurzeln von $f(x) = 0$ p geben, welche ein rationales Product haben; dieses kann man finden, wenn man die Gleichung bildet, deren sämmtliche Wurzeln Werthe des Productes von p Wurzeln sind; diese Gleichung muss dann eine rationale Wurzel haben; diese sei k; dann hat man

$$x_1 x_2 \dots x_p = k,$$

und erhält darauf die Coefficienten des rationalen Factors als Functionen von k. Falls die Gleichung in k gleiche Wurzeln hat, kann man von einer anderen symmetrischen Function der p Wurzeln ausgehen, z. B.

$$y = (\alpha - x_1)(\alpha - x_2) \dots (\alpha - x_p),$$

worin, wie man leicht sieht, α immer so gewählt werden kann, dass man keine gleiche Wurzeln in der Gleichung in φ bekommt, wenn die gegebene Gleichung keine gleiche Wurzeln hat. Da k Factor des letzten Gliedes der Gleichung ist, kann man oft, wenn dieses nur wenige Factoren hat, mit diesen probeweise vorgehen um die beschwerliche Bildung der Gleichung in k zu vermeiden.

Wenn k rational ist, muss es einen rationalen Factor geben, falls k nicht mehrfache Wurzel ist; ist k dagegen mehrfache Wurzel, so muss nicht nothwendig ein rationaler Factor vom p^{ten} Grade vorhanden sein, da die beiden Gleichungen (7) in diesem Falle einen gemeinschaftlichen Factor von höherem als dem p^{ten} Grade erhalten. Später wird zu diesem Fall zurückgekehrt werden; hier soll nur noch bemerkt werden, dass es nach dem Voranstehenden *immer möglich ist, eine gegebene reductible Gleichung in irreductible Gleichungen zu zerlegen.*

Sechstes Kapitel.

Abelsche Gleichungen.

Gleichungen, in denen eine Wurzel rational durch eine andere Wurzel ausgedrückt werden kann.

77. Gauss hat gezeigt, dass die Gleichungen, welche die Theilung der Kreisperipherie bestimmen, immer algebraisch auflösbar sind; diese Klasse von Gleichungen ist mit einbegriffen in einer umfassenderen Klasse, welche Abel später untersucht hat, und welche den Namen *Abelsche Gleichungen* erhalten haben; es sind solche Gleichungen, in denen eine Wurzel als eine rationale Function einer anderen Wurzel ausgedrückt werden kann. Hierher gehören z. B. die reciproken Gleichungen und Gleichungen dritten Grades (54. Aufgabe). Die Abelschen Gleichungen können immer auf Gleichungen von niedrigerem Grade reducirt werden und sind in gewissen Fällen algebraisch auflösbar.

In der irreductiblen Gleichung n^{ten} Grades

$$f(x) = 0 \quad \ldots\ldots\ldots\ldots \quad (1)$$

werde angenommen, dass für zwei der Wurzeln

$$x_1 = \theta(x_2) \quad \ldots\ldots\ldots\ldots \quad (2)$$

sei, wo θ eine rationale Function bedeutet.

Bildet man die Gleichung in y, deren Wurzeln bestimmt werden durch

$$y_1 = \theta(x_1);\ y_2 = \theta(x_2) \ldots y_n = \theta(x_n), \quad \ldots\ldots\ldots (3)$$

so erhält man eine Gleichung, welche dieselben Wurzeln haben muss, wie die gegebene. Sie ist nämlich von demselben Grade wie die gegebene, und da $\theta(x_2) = y_2 = x_1$, haben die beiden Gleichungen eine Wurzel gemeinschaftlich und müssen deshalb, da $f(x) = 0$ irreductibel ist, alle Wurzeln gemeinschaftlich haben. Daraus folgt, dass, wenn man die durch θ angedeutete Operation an einer beliebigen Wurzel vornimmt, man zu einer anderen Wurzel gelangen muss. Wird diese auf dieselbe Weise behandelt und fährt man so fort, so muss man einmal zu einer Wurzel kommen, die man schon früher gehabt hat; eine Gruppe von Wurzeln, z. B. 3, müssen deshalb verbunden sein durch die Gleichungen

$$\left.\begin{array}{l} x_1 = \theta(x_2) \\ x_2 = \theta(x_3) \\ x_3 = \theta(x_1) \end{array}\right\} \quad \ldots\ldots\ldots (4).$$

Setzt man aus einer dieser Gleichungen in die andere ein, erhält man, wenn man $\theta[\theta(x)]$ mit $\theta^2(x)$ bezeichnet u. s. w.

$$x_1 = \theta^3(x_1). \quad \ldots\ldots\ldots (5)$$

Diese Gleichung kann nicht identisch sein, wenn man $\theta(x)$ als von ganzer Form annimmt, was immer möglich ist (26), und wenn man den früher behandelten Fall ausnimmt, wo θ linear ist; sie hat die Wurzel x_1 mit $f(x) = 0$ gemeinschaftlich und wird deshalb von allen Wurzeln derselben befriedigt; nimmt man eine von den übrigen Wurzeln der Gleichung, x_4, so muss diese mit zwei anderen der Wurzeln eine ähnliche Gruppe bilden; in dieser Gruppe können nicht mehr als drei Wurzeln sein, denn die Gleichung

$$x_4 = \theta^3(x_4)$$

zeigt, dass man, nachdem man die durch θ bezeichnete Operation drei Male ausgeführt hat, wiederum x_4 erhalten hat; weniger als drei können es nicht sein, denn dann müsste

man z. B. $x_4 = \theta^2(x_4)$ haben, aber daraus würde $x_1 = \theta^2(x_1)$ folgen, und dann würde die erste Gruppe auch nur zwei Wurzeln enthalten. Dieselbe Wurzel kann nicht in zwei Gruppen vorkommen, denn wenn die zweite Gruppe z. B. x_4, x_5 und x_1 enthielte, hätte man sowohl

$$\theta(x_1) = x_3 \text{ als auch } \theta(x_1) = x_5,$$

folglich

$$x_3 = x_5,$$

welches unmöglich ist, da die gegebene Gleichung, weil irreductibel, keine gleichen Wurzeln haben kann.

Man sieht also, *dass die Wurzeln sich in Gruppen mit gleich vielen in jeder Gruppe vertheilen lassen. Wenn n eine Primzahl ist, müssen die Wurzeln deshalb alle eine einzige Gruppe bilden;* ist n eine zusammengesetzte Zahl, so muss diese durch die Anzahl der Wurzeln in jeder Gruppe theilbar sein.

Hat man nun z. B. m Gruppen, jede von p Wurzeln, so muss $n = mp$ sein. *Die Gleichung kann in diesem Falle aufgelöst werden mit Hülfe einer Gleichung vom p^{ten} Grade, deren Coefficienten durch eine Gleichung m^{ten} Grades bestimmt werden.*

Nimmt man der Einfachheit wegen den oben betrachteten Fall, wo $p = 3$, kann man

$$y_1 = x_1 + x_2 + x_3 = \theta^2(x_3) + \theta(x_3) + x_3 \quad \ldots\ldots \quad (6)$$

setzen. Indem x_3 auf alle möglichen Arten aus den Wurzeln der gegebenen Gleichung entnommen wird, erhält y 3m Werthe; von diesen stimmen indessen drei und drei überein, indem man z. B. hat

$$\theta^2(x_2) + \theta(x_2) + x_2 = x_3 + x_1 + x_2.$$

$$\theta^2(x_1) + \theta(x_1) + x_1 = x_2 + x_3 + x_1;$$

y hat also nur m Werthe und wird deshalb durch eine Gleichung m^{ten} Grades mit rationalen Coefficienten bestimmt.

Man kann diese mit Hülfe der Theorie der symmetrischen Functionen bilden oder dadurch, dass man x aus

$$f(x) = 0 \text{ und } y = x + \theta(x) + \theta^2(x) \quad \dots\dots\dots (7)$$

eliminirt.

Diese Gleichung

$$\varphi(y) = 0 \quad \dots\dots\dots (8)$$

vom m^{ten} Grade hat also die Wurzeln

$$\left.\begin{array}{l} y_1 = x_1 + x_2 + x_3 \\ y_2 = x_4 + x_5 + x_6 \\ \dots\dots\dots \\ \dots\dots\dots \\ y_m = x_{3m-2} + x_{3m-1} + x_{3m} \end{array}\right\} \quad \dots\dots\dots (9).$$

Falls nun alle diese Wurzeln ungleich gross sind, kann man die allgemeine Form finden für einen Factor dritten Grades von f(x),

$$x^3 - y_p x^2 + \Psi_1(y_p) x + \Psi_2(y_p);$$

setzt man hier für y_p nach und nach $y_1, y_2 \dots y_m$, so erhält man die m Factoren dritten Grades von f(x). Die gegebene Gleichung vom Grade 3m ist dergestalt auf die beiden Gleichungen

$$\left.\begin{array}{c} x^3 - y x^2 + \Psi_1(y) x + \Psi_2(y) = 0 \\ \varphi(y) = 0 \end{array}\right\} \quad \dots\dots\dots (10).$$

reducirt, von denen die erste vom dritten, die zweite vom m^{ten} Grade ist. Dieselbe Betrachtung kann angewendet werden, wenn man in jeder Gruppe statt der drei eine beliebige Anzahl von Wurzeln hat.

Die Gleichung $\varphi(y) = 0$ giebt zu besonderen Bemerkungen keinen Anlass; sie kann beliebig sein; die andere Gleichung ist dagegen wiederum eine Abelsche, da alle ihre Wurzeln eine Gruppe mit der oben angegebenen characteristischen Eigenschaft bilden; weiter unten wird bewiesen werden, dass sie immer algebraisch auflösbar ist.

78. Es ist möglich, dass $\varphi(y) = 0$ gleiche Wurzeln habe; in diesem Falle kann man ausgehen von der Function

$$y_I = (\alpha - x_1)(\alpha - x_2)(\alpha - x_3) = \left(\alpha - \theta^2(x_3)\right)\left(\alpha - \theta(x_3)\right)(\alpha - x_3), \quad (11)$$

worin α immer so gewählt werden kann, dass zwei Werthe von y nicht gleich gross werden können; hätte man nämlich für alle Werthe von α z. B. $y_1 = y_2$ oder

$$(\alpha - x_1)(\alpha - x_2)(\alpha - x_3) = (\alpha - x_4)(\alpha - x_5)(\alpha - x_6),$$

müssten die drei Wurzeln der ersten Gruppe dieselben sein wie die drei Wurzeln der zweiten Gruppe, wodurch die gegebene Gleichung reductibel würde.

Das Resultat dieser Untersuchung ist also folgendes: *Wenn p von den Wurzeln einer irreductiblen Gleichung ausgedrückt werden können durch x_1, $\theta(x_1)$, $\theta^2(x_1) \ldots \theta^{p-1}(x_1)$, wo θ so beschaffen ist, dass $\theta^p(x_1) = x_1$, so muss die Gleichung vom Grade mp sein, und kann dann mit Hülfe einer Gleichung vom m^{ten} Grade auf eine Gleichung p^{ten} Grades reducirt werden.*

Abelsche Gleichungen, deren Wurzeln eine Gruppe bilden.

79. Es bleibt noch übrig, die Gleichung vom n^{ten} Grade

$$f(x) = 0 \ldots\ldots\ldots\ldots \quad (1)$$

zu betrachten, deren Wurzeln ausgedrückt werden können durch

$$x_1,\ \theta(x_1),\ \theta^2(x_1), \ldots \theta^{n-1}(x_1), \ldots\ldots\ldots \quad (2)$$

wo x_1 eine beliebige der Wurzeln ist und

$$\theta^n(x_1) = x_1 \ldots\ldots\ldots\ldots \quad (3)$$

Wird eine beliebige Wurzel der Gleichung

$$x^n = 1 \ldots\ldots\ldots\ldots \quad (4)$$

durch α bezeichnet, so wird die Grösse

$$\Psi(x_1) = \left[x_1 + \alpha\,\theta(x_1) + \alpha^2\,\theta^2(x_1) + \ldots \alpha^{n-1}\,\theta^{n-1}(x_1)\right]^n, \;.\;.\; (5)$$

worin α als bekannt betrachtet wird, nur einen Werth haben, und folglich rational ausgedrückt werden können durch die Coefficienten der gegebenen Gleichung, die Coefficienten in θ und α.

Nimmt man nämlich statt x_1 eine andere der Wurzeln, z. B. $x_3 = \theta^2(x_1)$, so erhält man

$$\Psi(x_3) = \left[\theta^2(x_1) + \alpha\,\theta^3(x_1) + \alpha^2\,\theta^4(x_1) + \ldots + \alpha^{n-1}\,\theta(x_1)\right]^n,$$

wo die Grösse zwischen den Klammern aus der oben in Klammern eingeschlossenen Grösse durch Multiplication mit α^{n-2} gebildet wird. Da nun $\alpha^n = 1$, werden die beiden Grössen auf die n^{te} Potenz erhoben dasselbe Resultat geben.

Da auf diese Weise gezeigt, dass

$$\Psi(x_1) = \Psi(x_2) \ldots = \Psi(x)_n, \;.\;.\;.\;.\;.\;.\;.\;.\;.\;.\; (6)$$

kann man

$$\Psi(x_1) = \frac{1}{n}\left[\Psi(x_1) + \Psi(x_2) + \ldots \Psi(x_n)\right] \;.\;.\;.\;.\;.\;.\; (7)$$

setzen und dergestalt die symmetrische Function Ψ berechnen. Diese enthält α und bekommt deshalb einen Werth für jeden der n verschiedenen Werthe, welche α beigelegt werden können.

Wird der α_r entsprechende Werth von Ψ mit υ_r bezeichnet, erhält man n Gleichungen von der Form

$$x + \alpha_r\,\theta(x) + \alpha_r^2\,\theta^2(x) + \ldots \alpha_r^{n-1}\,\theta^{n-1}(x) = \sqrt[n]{\upsilon_r} \;.\;.\;.\;.\; (8)$$

Der $\alpha_r = 1$ entsprechende Werth von $\sqrt[n]{\upsilon_r}$ ist bekannt, da die Summe der Wurzeln bekannt ist; derselbe wird $-A$, wenn A der Coefficient von x^{n-1} ist. Addirt man nun die n Gleichungen und beachtet, dass

$$\Sigma\,\alpha^p = 0$$

für alle Werthe von p, welche nicht theilbar sind durch n, so erhält man, wenn $\alpha_0 = 1$ genommen wird,

$$x = \frac{-A + \sqrt[n]{\upsilon_1} + \sqrt[n]{\upsilon_2} + \ldots \sqrt[n]{\upsilon_{n-1}}}{n} \quad \ldots\ldots\ldots (9)$$

Multiplicirt man vor der Addition jede der Gleichungen mit α_r^{-m}, fallen bei der Addition alle Glieder auf der linken Seite fort, ausgenommen $\theta^m(x)$; man erhält deshalb irgend eine beliebige der Wurzeln bestimmt durch

$$\theta^m(x) = \frac{-A + \alpha_1^{-m}\sqrt[n]{\upsilon_1} + \alpha_2^{-m}\sqrt[n]{\upsilon_2} + \ldots + \alpha_{n-1}^{-m}\sqrt[n]{\upsilon_{n-1}}}{n} \quad \ldots (10)$$

In diesem Ausdruck kann eine der Wurzelgrössen mit irgend einem beliebigen ihrer Werthe genommen werden, aber jede der übrigen muss mit einem bestimmten Werthe genommen werden, sobald der Werth der ersten festgesetzt ist. Es sei z. B. das in υ_1 vorkommende α eine primitive Wurzel der Einheit; die übrigen Werthe von α können dann als Potenzen von dieser dargestellt werden, z. B. $\alpha_p = \alpha^p$; dann hat man

$$\left.\begin{aligned} \sqrt[n]{\upsilon_1} &= x + \alpha\,\theta(x) + \alpha^2\,\theta^2(x) + \ldots \alpha^{n-1}\,\theta^{n-1}(x), \\ \sqrt[n]{\upsilon_p} &= x + \alpha^p\,\theta(x) + \alpha^{2p}\,\theta^2(x) + \ldots \alpha^{(n-1)p}\,\theta^{n-1}(x). \end{aligned}\right\} \quad \ldots (11)$$

Vertauscht man in diesen beiden Gleichungen x mit $\theta^m(x)$, so wird die erste mit α^{-m}, die zweite mit α^{-pm} multiplicirt. Das Product

$$\varphi(x) = \left(\sqrt[n]{\upsilon_1}\right)^{n-p}\sqrt[n]{\upsilon_p} \quad \ldots\ldots\ldots\ldots (12)$$

wird deshalb multiplicirt mit

$$\alpha^{-m(n-p)}\,\alpha^{-mp} = \alpha^{-mn} = 1,$$

dass heisst, es bleibt unverändert bei der Vertauschung von zweien der Werthe von x; $\varphi(x)$ ist deshalb eine rationale Function, welche wie vorhin $\Psi(x)$ berechnet werden kann; bezeichnet man den Werth derselben mit a_p, erhält man also

$$\sqrt[n]{\upsilon_p} = \frac{a_p}{\upsilon_1}\left(\sqrt[n]{\upsilon_1}\right)^p \quad \ldots\ldots\ldots\ldots\ldots (13)$$

Alle Wurzelgrössen in x können deshalb rational durch eine derselben ausgedrückt werden; werden diese Ausdrücke in (9) eingesetzt, erhält man für x einen Ausdruck, der nur n Werthe hat, entsprechend den n Werthen von $\sqrt[n]{\upsilon_1}$. Im Resultate kommt α vor, welches sich, wie später gezeigt werden wird, immer algebraisch ausdrücken lässt. Das Resultat der geführten Untersuchung ist deshalb, dass *eine Gleichung n^{ten} Grades, deren Wurzeln $x, \theta(x), \theta^2(x) \ldots \theta^{n-1}(x)$ sind, wo $\theta^n(x) = x$, immer algebraisch auflösbar ist.* Da diese Eigenschaft, *wenn n eine Primzahl ist,* sich immer bei *Gleichungen findet, bei denen eine Wurzel eine rationale Function einer anderen Wurzel ist*, *können solche Gleichungen immer algebraisch aufgelöst werden.*

Falls die Coefficienten in f und θ reell sind, wird α die einzige complexe Grösse in υ_1, und da die Werthe von α paarweise conjugirt sind, nämlich α^k und α^{n-k}, muss dasselbe für die Werthe von υ gelten; man erhält dann z. B.

$$\left.\begin{array}{l} \upsilon_1 = \rho\,(\cos\omega + i\sin\omega) \\ \upsilon_{n-1} = \rho\,(\cos\omega - i\sin\omega) \end{array}\right\}, \ldots\ldots\ldots\ldots \quad (14)$$

worin (12)

$$\rho^2 = \upsilon_1\,\upsilon_{n-1} = a_{n-1}^n. \ldots\ldots\ldots\ldots \quad (15)$$

Da $a_{n-1} = \sqrt[n]{\upsilon_1}\,\sqrt[n]{\upsilon_{n-1}}$ nicht verändert wird, wenn man α mit α^{n-1} vertauscht, und keine anderen complexen Grössen als α enthält, muss diese Grösse reell sein. Man erhält nun

$$\sqrt[n]{\upsilon_1} = \sqrt{a}\left(\cos\frac{2p\pi + \omega}{n} + i\sin\frac{2p\pi + \omega}{n}\right), \ldots \quad (16)$$

worin a den numerischen Werth der Grösse a_{n-1} bedeutet; hieraus folgt wiederum

$$\sqrt[n]{\upsilon_k} = \frac{a_k}{\upsilon_1}\sqrt{a^k}\left(\cos\frac{k(2p\pi + \omega)}{n} + i\sin\frac{k(2p\pi + \omega)}{n}\right), \quad (17)$$

so dass die Wurzeln ausser von rationalen Grössen nur abhängen von einer Quadratwurzel, sin. und cos. von $\frac{1}{n}$ der

Kreisperipherie und $\frac{1}{n}$ eines Winkels ω, dessen tg. eine rationale Function der genannten sin. und cos. ist.

Da θ reell ist, sieht man zugleich, dass *wenn eine der Wurzeln reell ist, alle reell sein müssen,* so dass sie also entweder alle reell oder alle complex sind.

Ueber den Fall, wo der Grad der Gleichung keine Primzahl ist.

80. Die für die Auflösung der Abelschen Gleichung, in der alle Wurzeln eine Gruppe bilden, dargelegte Methode kann in allen Fällen angewendet werden, aber wenn der Grad der Gleichung nicht durch eine Primzahl angegeben wird, kann man die Auflösung vereinfachen.

Es sei $n = mp$; man kann dann die Wurzeln in m Gruppen von je p Wurzeln theilen, nämlich

$$\left.\begin{array}{l} x,\ \theta^m(x),\ \theta^{2m}(x), \ldots \theta^{(p-1)m}(x) \\ \theta(x),\ \theta^{m+1}(x),\ \theta^{2m+1}(x), \ldots \theta^{(p-1)m+1}(x) \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \theta^{m-1}(x),\ \theta^{2m-1}(x), \ldots \theta^{pm-1}(x) \end{array}\right\} \ldots\ldots (1)$$

Setzt man nun

$$\theta^m(x) = \theta_1(x), \ldots\ldots (2)$$

werden die Wurzeln der ersten Reihe

$$x,\ \theta_1(x),\ \theta_1{}^2(x), \ldots \theta_1^{p-1}(x), \ldots\ldots (3)$$

wo

$$\theta_1{}^p(x) = \theta^{mp}(x) = x. \ldots\ldots (4)$$

Man kann nun zufolge 77 die Gleichung mit Hülfe einer Gleichung m^{ten} Grades auf eine Gleichung vom p^{ten} Grade reduciren. Die Gleichung vom p^{ten} Grade hat dieselbe Eigenschaft wie die gegebene; dieses galt bei dem in 77 und

78 behandelten Falle nicht von der Gleichung m^{ten} Grades, aber man kann beweisen, dass es hier, wo alle Wurzeln eine Gruppe bilden, gilt, so dass die beiden Gleichungen, auf welche die gegebene Gleichung zurückgeführt wird, die Eigenschaft derselben behalten.

Die Gleichung vom m^{ten} Grade in y ist so beschaffen, dass eine ihrer Wurzeln eine symmetrische Function von den p Wurzeln der ersten Gruppe ist; die übrigen Wurzeln sind in derselben Weise abhängig von den Wurzeln in den übrigen Gruppen.

Nun sei y_1 die Wurzel, welche aus

$$x, \theta^m(x), \theta^{2m}(x) \ldots \theta^{(p-1)m}(x) \ldots\ldots\ldots\ldots (5)$$

gebildet wird und y_2 diejenige, welche gebildet wird aus

$$\theta(x), \theta^{m+1}(x), \theta^{2m+1}(x) \ldots \theta^{(p-1)m+1}(x). \ldots\ldots (6)$$

Die Coefficienten der Gleichung, welche die Wurzeln (5) bestimmt, sind rationale Functionen von y_1, und folglich können alle symmetrischen Functionen dieser Wurzeln rational durch y_1 ausgedrückt werden. y_2 ist inzwischen eine symmetrische Function von

$$\theta(x), \theta . \theta^m(x), \theta . \theta^{m}(x) \ldots$$

und folglich auch von den Wurzeln (5). y_2 kann also rational durch y_1 ausgedrückt werden, so dass die Gleichung in y dieselbe Eigenschaft hat wie die gegebene.

Sind m und p zusammengesetzte Zahlen, kann man auf dieselbe Weise fortfahren; *jede Abelsche Gleichung, deren Wurzeln eine Gruppe bilden, kann deshalb auf Abelsche Gleichungen reducirt werden, deren Grade durch eine Primzahl angegeben werden.*

Ueber irreductible Gleichungen, in welchen zwei Wurzeln verbunden sind durch die Relation

$$x_1 x_2 + a x_1 + b x_2 + c = 0. \quad \ldots \ldots \quad (1)$$

81. Von a, b und c wird angenommen, dass sie gegebene Grössen seien, und zwar rationale Functionen von solchen Grössen, von denen die Coefficienten der Gleichung wiederum rationale Functionen sind. Vertauscht man in der Gleichung x mit $x + h$, wo h bestimmt wird durch die Gleichung

$$h^2 + (a + b) h + c = 0, \quad \ldots \ldots \quad (2)$$

werden zwei Wurzeln der neuen Gleichung verbunden durch die Relation

$$x_1 x_2 + (h + a) x_1 + (h + b) x_2 = 0. \quad \ldots \ldots \quad (3)$$

Vertauscht man wiederum x mit $\frac{1}{x}$, erhält man für zwei Wurzeln der neuen Gleichung

$$1 + (h + a) x_2 + (h + b) x_1 = 0. \quad \ldots \ldots \quad (4)$$

Wird endlich x mit $x + h_1$ vertauscht, wo

$$(2h + b + a) h_1 + 1 = 0, \quad \ldots \ldots \quad (5)$$

erhält man eine neue Gleichung, in der zwei Wurzeln verbunden sind durch die Relation

$$x_1 = \alpha x_2, \text{ wo } \alpha = -\frac{h + a}{h + b}. \quad \ldots \ldots \quad (6)$$

Nun nehme man an, dass die gegebene Gleichung fortfährt irreductibel zu bleiben, selbst wenn h, welches durch eine Gleichung zweiten Grades bestimmt wird, als eine bekannte Grösse betrachtet wird, welche bei der Zerlegung in Factoren benutzt werden kann; in diesem Falle muss die zuletzt gebildete Gleichung auch irreductibel sein, denn wenn sie sich in mehrere andere zerlegen liesse, brauchte man nur in diese wiederum die ursprüngliche Unbekannte einzuführen,

um dadurch die gegebene Gleichung zu zerlegen. Eine Gruppe von Wurzeln muss dann die Beziehungen

$$x_1 = \alpha x_2,\ x_2 = \alpha x_3 \ldots x_p = \alpha x_1 \ \ldots\ldots\ldots \ (7)$$

haben, welche zeigen, dass α eine primitive Wurzel der Gleichung

$$\alpha^p = 1 \ \ldots\ldots\ldots\ldots\ldots\ldots \ (8)$$

sein muss. Aus

$$\alpha = -\frac{h + a}{h + b} \ \ldots\ldots\ldots\ldots\ldots\ldots \ (9)$$

erhält man nun

$$h = -\frac{a + b\alpha}{1 + \alpha}; \ \ldots\ldots\ldots\ldots\ldots \ (10)$$

dieses in (2) eingesetzt giebt

$$\alpha^2 (ab - c) + (a^2 + b^2 - 2c)\alpha + ab - c = 0 \ \ldots\ldots \ (11)$$

Die zweite Wurzel dieser Gleichung muss die zu α gehörige conjugirte sein, da das Product der Wurzeln 1 ist. Schreibt man diese Wurzeln nun

$$\cos \upsilon + i \sin \upsilon$$

und

$$\cos \upsilon - i \sin \upsilon,$$

erhält man

$$2 \cos \upsilon = \frac{a^2 + b^2 - 2c}{c - ab} = \frac{(a - b)^2}{c - ab} - 2$$

oder

$$c = ab + \frac{(a - b)^2}{4 \cos^2 \frac{\mu\pi}{p}}; \ h = \frac{a + b}{2} \pm i \frac{a - b}{2} \operatorname{tg} \frac{\mu\pi}{p}, \ \ldots \ (12)$$

wo μ prim zu p ist, da α eine primitive Wurzel sein soll.

Man sieht, dass eine Gruppe von p Wurzeln der transformirten Gleichung durch eine derselben ausgedrückt werden kann; nennt man diese y_1, so werden alle p durch die Gleichung

$$x^p - y_1^p = 0$$

bestimmt, und wenn es m solcher Gruppen giebt, muss man die Gleichung darstellen können unter der Form

$$(x^p - y_1^p)(x^p - y_2^p) \dots (x^p - y_m^p) = 0. \quad \dots\dots (13)$$

$y_1^p, y_2^p, \dots y_m^p$ können also als Wurzeln einer beliebigen Gleichung m^{ten} Grades betrachtet werden; ist diese

$$f(y) = 0, \quad \dots\dots\dots\dots\dots\dots (14)$$

wird die Gleichung in x

$$f(x^p) = 0 \quad \dots\dots\dots\dots\dots\dots (15)$$

sein, und die gegebene Gleichung muss dann so beschaffen sein, dass sie durch die angegebenen einfachen Transformationen auf diese Form gebracht werden kann. Man sieht leicht, dass p als Primzahl angenommen werden kann, ohne dass die Auflösung weniger allgemein wird.

82. Bei Gleichungen mit der hier angegebenen allgemeinen Form, wird die zwischen den Wurzeln bestehende Relation (1) α enthalten; soll die Relation nur rationale gegebene Grössen enthalten, muss

$$\cos^2 \frac{\mu\pi}{p}$$

rational sein, dass heisst, es muss die Primzahl p gleich 2 oder 3 sein.

Für $p = 2$ ist der Ausdruck für c unbrauchbar; man hat indessen in diesem Falle

$$\alpha = -1 = -\frac{h + a}{h + b},$$

also

$$a = b,$$

wodurch die Relation

$$x_1 x_2 + a(x_1 + x_2) + c = 0 \quad \dots\dots\dots\dots (16)$$

wird. Setzt man

$$y = x_1 + x_2,$$

findet man die Gleichung in y durch Elimination von x aus der gegebenen Gleichung und

$$x^2 - yx - ay - c = 0.$$

Dass die Gleichung zu dieser Klasse gehört zeigt sich dadurch, dass sie unverändert bleibt, wenn man an Stelle von x

$$-\frac{ax + c}{x + a}$$

setzt.

Umgekehrt findet man alle Gleichungen dieser Klasse vom Grade 2n, wenn man in der allgemeinen Gleichung in y vom n^{ten} Grade

$$y = \frac{x^2 - c}{x + a} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (17)$$

setzt.

Für $p = 3$ hat man

$$c = ab + (a - b)^2, \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (18)$$

also die Relation

$$x_1 x_2 + a x_1 + b x_2 + ab + (a - b)^2 = 0. \quad \ldots\ldots \quad (19)$$

Diese Gleichungen müssen also unverändert bleiben wenn man für x

$$-\frac{ax + a^2 - ab + b^2}{x + b} \quad \ldots\ldots\ldots\ldots\ldots \quad (20)$$

einsetzt; sie werden auf Gleichungen von der Form

$$x'^3 = y$$

reducirt, wo

$$x' = \frac{1}{x - h} + \frac{1}{2h + a + b}; \; x = h + \frac{2h + (a + b)}{(2h + a + b)x' - 1} \quad (21)$$

und

$$\left.\begin{aligned} h &= -\frac{a + b}{2} \pm \frac{a - b}{2}\sqrt{-3} \\ &= -a \pm (a - b)\alpha \end{aligned}\right\} \quad \ldots\ldots\ldots \quad (22)$$

Man kann die Coefficienten der Gleichung dritten Grades leicht durch einen derselben ausdrücken; setzt man

$$x_1 + x_2 + x_3 = -y;\; x_1 x_2 + x_1 x_3 + x_2 x_3 = a_2;\; x_1 x_2 x_3 = -a_3,$$

so erhält man aus

$$\begin{aligned} x_1 x_2 + a x_1 + b x_2 + a^2 - a b + b^2 &= 0, \\ x_2 x_3 + a x_2 + b x_3 + a^2 - a b + b^2 &= 0, \\ x_3 x_1 + a x_3 + b x_1 + a^2 - a b + b^2 &= 0 \end{aligned}$$

durch Addition

$$a_2 - (a + b) y + 3 (a^2 - a b + b^2) = 0,$$

und durch Addition, nachdem die Gleichungen beziehungsweise mit x_3, x_1 und x_2 multiplicirt worden sind

$$-3 a_3 + (a + b) a_2 - y (a^2 - a b + b^2) = 0;$$

dadurch wird die Gleichung

$$x^3 + y x^2 + [(a + b) y - 3 (a^2 - a b + b^2)] x + a b y - (a^3 + b^3) = 0. \quad (23)$$

Durch Elimination von y aus dieser Gleichung und

$$F(y) = 0, \ldots\ldots\ldots\ldots \quad (24)$$

wo $F(y) = 0$ eine beliebige irreductible Gleichung ist, bildet man eine Gleichung von der hier untersuchten Art.

Beisp.

$$x^3 + x^2 - 2x - 1 = 0.$$

Diese Gleichung bleibt unverändert, wenn man x mit $-\frac{1}{1+x}$ vertauscht; man hat deshalb

$$x_1 x_2 + x_1 + 1 = 0,$$

also

$$a = 1;\; b = 0;\; h = \alpha;\; h_1 = -\frac{1}{1 + 2\alpha} = \frac{1 + 2\alpha}{3}.$$

Die reducirte Gleichung wird

$$x'^3 = \frac{\pm 13\sqrt{-3} - 9}{126}.$$

83. Es wurde oben vorausgesetzt, dass die gegebene Gleichung irreductibel bleibt, wenn die in h vorkommende Quadratwurzel als bekannt eingeführt wird; wird diese Quadratwurzel k genannt, so ist es indessen möglich, dass die gegebene Gleichung in zwei Gleichungen

$$A + kB = 0$$

und

$$A - kB = 0$$

zerlegt werden kann; indessen ist es einleuchtend, dass auch in diesem Falle die Relation (1) x_2 als eine Wurzel in einer dieser Gleichungen bestimmt, wenn x_1 als eine andere der Wurzeln genommen wird.

Die transformirte Gleichung lässt sich nun auch in zwei andere zerlegen, aber von diesen gilt, dass jede Wurzel x_k durch eine andere Wurzel x_1 bestimmt wird durch die Relation

$$x_k = \alpha x_1.$$

Man gelangt dann zu derselben Bestimmung von α wie in dem allgemeinen Falle, so dass sich folgender allgemeine Satz aufstellen lässt:

Sind zwei Wurzeln einer irreductiblen Gleichung n^{ten} Grades durch die Relation (1) verbunden, so lässt sich die Gleichung auf eine Gleichung zweiten Grades mit Hülfe *einer Gleichung vom Grade* $\frac{n}{2}$ *reduciren falls* $a = b$*; im entgegengesetzten Falle lässt sie sich auf eine Gleichung dritten Grades mit Hülfe einer Gleichung vom Grade* $\frac{n}{3}$ *reduciren. In letzterem Falle muss* $c = a^2 - ab + b^2$ *sein.*

84. Wenn zwei Wurzeln einer irreductiblen Gleichung bei der Entwicklung in gemeine Kettenbrüche mit demselben vollständigen Quotienten abschliessen, muss die Gleichung zu der hier untersuchten Klasse gehören. Wird

der gemeinschaftliche vollständige Quotient q genannt, erhält man nämlich

$$x_1 = \frac{d + d_1 q}{e + e_1 q}; \; x_2 = \frac{f + f_1 q}{g + g_1 q}, \quad \ldots \ldots \ldots (25)$$

indem $\frac{d}{e}$ und $\frac{d_1}{e_1}$ die beiden letzten Näherungswerthe von x_1, $\frac{f}{g}$ und $\frac{f_1}{g_1}$ die beiden letzten Näherungswerthe von x_2 sind, welche man erhält, wenn man die verschiedenen Theile der Kettenbrüche benutzt. Wird q eliminirt, erhält man

$$(e g_1 - g e_1) x_1 x_2 + (e_1 f - e f_1) x_1 + (d_1 g - d g_1) x_2 + d f_1 - d_1 f = 0. \quad (26)$$

Man hat nun identisch

$$(e_1 f - e f_1)(d_1 g - d g_1) + (d e_1 - e d_1)(f g_1 - g f_1) = (e g_1 - g e_1)(d f_1 - f d_1), \quad \ldots . (27)$$

wo wie bekannt

$$\left. \begin{array}{l} d e_1 - e d_1 = \pm 1 \\ f g_1 - g f_1 = \pm 1 \end{array} \right\} \ldots \ldots \ldots \ldots \ldots (28)$$

Für $p = 2$, $(a = b)$ und wenn man

$$e g_1 - g e_1 = \lambda, \; e_1 f - e f_1 = d_1 g - d g_1 = a$$

setzt, giebt (27)

$$d f_1 - d_1 f = \frac{a^2 \pm 1}{\lambda},$$

wo λ ein Factor von $a^2 \pm 1$ sein muss; die allgemeine Form für eine Gleichung mit den Wurzeln x_1 und x_2 ist dann

$$x^2 - y x - \frac{a y}{\lambda} - \frac{a^2 \pm 1}{\lambda^2} = 0, \quad \ldots \ldots \ldots (29)$$

worin a eine willkürliche ganze Zahl bedeutet, λ einen Factor von $a^2 \pm 1$ und y eine Wurzel einer beliebigen Gleichung.

Für $p = 3$ erhält man aus (27), wenn

$$e_1 f - e f_1 = a; \; d_1 g - d g_1 = b \text{ und } d f_1 - d_1 f = c$$

gesetzt wird

$$a b \pm 1 = \lambda c,$$

während man zugleich hat ((18))

$$\lambda c = a^2 - a b + b^2;$$

hieraus folgt

$$(b - a)^2 = \pm 1,$$

so dass man das obere Vorzeichen gebrauchen muss; man hat dann

$$b = a \pm 1,$$

$$c = \frac{a^2 \pm a + 1}{\lambda}.$$

Die allgemeine Form für eine Gleichung dritten Grades mit den Wurzeln x_1 und x_2 wird dann

$$\left.\begin{aligned} & x^3 + y x^2 + a_2 x + a_3 = 0, \\ & \text{worin} \\ & a_2 = \frac{2a \pm 1}{\lambda} y - \frac{3(a^2 \pm a + 1)}{\lambda^2} \\ & a_3 = \frac{a^2 \pm a}{\lambda^2} - \frac{(2a \pm 1)(a^2 \pm a + 1)}{\lambda^3} \end{aligned}\right\}; \quad \ldots\ldots \quad (30)$$

a ist eine willkürliche ganze Zahl und λ ein Factor von $a^2 \pm a + 1$.

Algebraische Auflösung der binomischen Gleichung.

85. Es ist gezeigt worden, dass die Auflösung binomischer Gleichungen auf die Auflösung von Gleichungen von der Form

$$x^p - 1 = 0, \quad \ldots\ldots\ldots\ldots \quad (1)$$

wo p eine Primzahl ist, reducirt wird; die Wurzeln dieser Gleichung wurden unter trigonometrischer Form dargestellt; nun soll gezeigt werden, wie dieselben immer unter algebraischer Form dargestellt werden können. Da zwei

Wurzeln der Gleichung (1) zur Summe $2\cos\frac{2\pi}{p}$ haben, wird die Kreisperipherie mittelst Zirkel und Lineal in p gleich grosse Theile getheilt werden können, sobald (1) durch Ausziehen von Quadratwurzeln aufgelöst werden kann. Dividirt man durch $x-1$, erhält man die irreductible Gleichung

$$x^{p-1}+x^{p-2}+\dots x^2+x+1=0, \quad \dots \dots \dots \quad (2)$$

deren Wurzeln, wenn eine derselben mit α bezeichnet wird, dargestellt werden können durch

$$\alpha, \alpha^r, \alpha^{r^2}, \dots \alpha^{r^{p-2}}, \quad \dots \dots \dots \quad (3)$$

wo r eine primitive Wurzel der Congruenz

$$x^{p-1}-1\equiv 0 \pmod{p} \quad \dots \dots \dots \quad (4)$$

ist, das heisst eine solche Zahl, dass p nicht in

$$r^k-1$$

aufgeht für irgend welchen niedrigeren Werth von k als $p-1$. Wie leicht ersichtlich bringt dies mit sich, dass alle Grössen in der Reihe (3) verschieden werden.

Nun sei β eine beliebige Wurzel (1 ausgenommen) der Gleichung

$$x^{p-1}-1=0; \quad \dots \dots \dots \quad (5)$$

es soll dann mit Rücksicht auf das Folgende das Product der beiden Grössen

$$\left.\begin{array}{l} V_1=\alpha+\beta\alpha^r+\beta^2\alpha^{r^2}+\dots+\beta^{p-2}\alpha^{r^{p-2}} \\ \text{und} \\ V_2=\alpha+\beta^{-1}\alpha^r+\beta^{-2}\alpha^{r^2}+\dots+\beta^{-(p-2)}\alpha^{r^{p-2}} \end{array}\right\} \quad \dots \quad (6)$$

gebildet werden.

Vereinigt man die Glieder des Productes, welche β^n enthalten, erhält man

$$\beta^n\left(\alpha^{r^n+1}+\alpha^{r(r^n+1)}+\alpha^{r^2(r^n+1)}+\dots+\alpha^{r^{p-2}(r^n+1)}\right).$$

Bezeichnet man α^{r^n+1}, welches eine der Wurzeln der gegebenen Gleichung ist, mit α_1, wird die Grösse in der Klammer

$$\alpha_1 + \alpha_1^r + \alpha_1^{r^2} + \ldots + \alpha_1^{r^{p-2}}.$$

Für den Fall, dass α_1 nicht 1 ist, hat man hier die Summe der Wurzeln von (2); diese Summe ist -1; ist dagegen $\alpha_1 = 1$, wird die Summe $p-1$; dieser Fall tritt ein, wenn

$$r^n + 1 \equiv 0 \pmod{p},$$

woraus

$$n = \frac{p-1}{2}.$$

Das gesuchte Product wird auf die Weise

$$-\left(1 + \beta + \beta^2 + \ldots + \beta^{p-2} - \beta^{\frac{p-1}{2}}\right) + (p-1)\beta^{\frac{p-1}{2}},$$

oder, da

$$1 + \beta + \beta^2 + \ldots + \beta^{p-2} = 0,$$

$$V_1 V_2 = p\beta^{\frac{p-1}{2}} = \pm p, \ldots\ldots\ldots\ldots\ldots \quad (7)$$

da entweder $\beta^{\frac{p-1}{2}} = +1$ oder $\beta^{\frac{p-1}{2}} = -1$.

In dem ersteren Falle kann man in den beiden Factoren V_1 und V_2 die Glieder zusammenziehen, welche um $\frac{p-1}{2}$ Stellen von einander entfernt sind; zwei solcher Glieder sind

$$\beta^n \alpha^{r^n} \text{ und } \beta^{n+\frac{p-1}{2}} \alpha^{r^{n+\frac{p-1}{2}}} = \beta^n \alpha^{-r^n},$$

indem

$$r^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

da p aufgeht in

$$\left(r^{\frac{p-1}{2}} - 1\right)\left(r^{\frac{p-1}{2}} + 1\right)$$

und nicht aufgeht in dem ersten Factor.

Die Summe S zweier solcher Glieder wird deshalb

$$S = \beta^n \left(\alpha^{r^n} + \alpha^{-r^n}\right)$$

oder, wenn z. B.

$$\alpha = \cos\frac{2\pi}{p} + i \sin\frac{2\pi}{p},$$

und wenn man

$$\frac{2\pi}{p} = a$$

setzt,

$$S = 2\beta^n \cos r^n a.$$

Die Formel wird dann, wenn man eine Wurzel der Gleichung

$$x^{\frac{p-1}{2}} - 1 = 0 \quad \dots\dots\dots\dots\dots\dots (8)$$

mit γ bezeichnet und $p = 2\mu + 1$ setzt,

$$4 V_1 V_2 = p \quad \dots\dots\dots\dots\dots\dots (9)$$

wo

$$V_1 = \cos a + \gamma \cos r a + \dots \gamma^{\mu-1} \cos r^{\mu-1} a,$$

$$V_2 = \cos a + \gamma^{-1} \cos r a + \dots \gamma^{-(\mu-1)} \cos r^{\mu-1} a.$$

86. Da die hier zu untersuchende Gleichung, wenn man

$$x^r = \theta(x)$$

setzt, die Wurzeln

$$x,\ \theta(x),\ \theta^2(x) \dots \theta^{p-2}(x)$$

hat, wo $\theta^{p-1}(x) = x$, gehört sie zu der in 79 untersuchten Klasse, so dass die Wurzeln derselben durch Summen von Gliedern von der Form

$$\sqrt[p-1]{\upsilon}$$

ausgedrückt werden können, wo υ eine rationale Function von den Coefficienten der Gleichung und von β ist. α kann deshalb durch Wurzelgrössen ausgedrückt werden, sobald dies

mit β der Fall ist; da die Bestimmung von β wiederum abhängig ist von binomischen Gleichungen, deren Grade durch Primzahlen kleiner als p bestimmt werden, muss man bei fortgesetzter Reduction endlich zu Gleichungen gelangen, deren Wurzeln bekannt sind und sich durch Wurzelgrössen ausdrücken lassen.

Von den Gliedern in α sind je zwei conjugirt, nämlich

$$\sqrt[p-1]{\upsilon_1} \text{ und } \sqrt[p-1]{\upsilon_{n-1}}$$

u. s. w. Diese beiden sind eben die Grössen V_1 und V_2, deren Product gleich $\pm p$ gefunden wurde. Ihr Modulus muss deshalb $\sqrt{p}$ sein. Die Argumente erhält man, indem man Winkel, welche construirt werden können, durch Primfactoren von $p - 1$ dividirt. Ist die Primzahl

$$p = 2^k + 1, \ldots \ldots \ldots \ldots \ldots \ldots \quad (10)$$

so enthält $p - 1$ keine anderen Primfactoren als 2. *Es bedarf also in diesem Falle, um mittelst Zirkel und Lineal eine Kreisperipherie in p gleich grosse Theile zu theilen, keiner anderen Constructionen, als der Construction rationaler Ausdrücke, der Halbirung von Winkeln und endlich der Construction einer Quadratwurzel* $\sqrt{p}$.

87. Anstatt die gegebene Gleichung so zu behandeln wie es hier geschehen ist, kann man ihre Eigenschaften als reciproke Gleichung benutzen um sie auf eine andere vom Grade μ zu reduciren. Diese behält den Character einer Abelschen Gleichung, da ihre Wurzeln die Summen von je zwei conjugirten Werthen von α werden; diese sind deshalb

$$2\cos a,\ 2\cos r\,a,\ 2\cos r^2 a \ldots 2\cos r^{\mu} a, \ldots \ldots \ldots \quad (11)$$

aber wie bekannt kann cos r a rational durch cos a ausgedrückt werden. Bildet man für diese Gleichung das Product

$$\sqrt[\mu]{\upsilon_1}\ \sqrt[\mu]{\upsilon_{n-1}},$$

gelangt man zu dem oben ((9)) bestimmten Product, dessen Werth gleich p gefunden wurde.

Gauss hat zuerst die hier behandelte Aufgabe gelöst; er zeigte, dass die Kreisperipherie in $p = 2^k + 1$ gleich grosse Theile getheilt werden könne, wenn diese Zahl eine Primzahl ist, und dass die Theilung ausgeführt werden könne durch Halbirung von Winkeln und Construction von $\sqrt{p}$. Abel hat dann später die Methode von Gauss verallgemeinert.

Theilung der Kreisperipherie in 17 gleich grosse Theile.

88. Die Theilung der Kreisperipherie in 17 gleiche Theile ist abhängig von der Gleichung

$$x^{17} - 1 = 0 \qquad (1)$$

Dividirt man durch $x - 1$ und reducirt die erhaltene reciproke Gleichung, gelangt man zu der Gleichung

$$x^8 + x^7 - 7x^6 - 6x^5 + 15x^4 - 10x^3 - 10x^2 - 4x + 1 = 0 \qquad (2)$$

Die Wurzeln dieser Gleichung sind

$$x = 2\cos\frac{2k\pi}{17} \qquad (3)$$

für $k = 1, 2 \ldots 8$.

Da die Gleichung (2) vom Grade 2^3 ist, kann sie nach der in 80 entwickelten Methode mit Hülfe von 3 Gleichungen zweiten Grades aufgelöst werden; indessen soll es vorgezogen werden, die ursprüngliche Gleichung vom 16ten Grade zu benutzen.

Die kleinste primitive Wurzel von $x^{16} \equiv 1 \pmod{17}$ ist 3; man setze deshalb $r = 3$ und erhält dadurch die Wurzeln

$$\alpha,\quad \alpha^3,\quad \alpha^9,\quad \alpha^{10},\quad \alpha^{13},\quad \alpha^5,\quad \alpha^{15},\quad \alpha^{11},$$

$$\alpha^{-1}, \alpha^{-3}, \alpha^{-9}, \alpha^{-10}, \alpha^{-13}, \alpha^{-5}, \alpha^{-15}, \alpha^{-11}.$$

Nun setze man

$$\left.\begin{array}{l} y_1 = \alpha + \alpha^9 + \alpha^{13} + \alpha^{15} + \alpha^{-1} + \alpha^{-9} + \alpha^{-13} + \alpha^{-15} \\ y_2 = \alpha^3 + \alpha^{10} + \alpha^5 + \alpha^{11} + \alpha^{-3} + \alpha^{-10} + \alpha^{-5} + \alpha^{-11} \end{array}\right\} \quad . . (4)$$

Dann hat man $y_1 + y_2 = -1$. Das Product $y_1 y_2$ muss rational sein, denn vertauscht man α mit einer beliebigen anderen Wurzel, so bleibt es unverändert; vertauscht man nämlich α mit einer Wurzel derselben Gruppe, wird weder y_1 noch y_2 verändert, und vertauscht man α mit einer Wurzel der anderen Gruppe, werden nur y_1 und y_2 vertauscht. Da nun das Product von zwei Wurzeln selber eine Wurzel ist, wird $y_1 y_2$ eine Summe von 64 Wurzeln; unter diesen kann 1 nicht vorkommen, da zwei conjugirte Wurzeln stets in derselben Gruppe stehen. Da das Product eine symmetrische Function der 16 Wurzeln ist, muss jede derselben vier Male vorkommen. Da nun die Summe der Wurzeln -1 ist, wird

$$y_1 y_2 = -4,$$

so dass y_1 und y_2 Wurzeln der Gleichung

$$y^2 + y - 4 = 0 \quad \ldots\ldots\ldots\ldots\ldots (5)$$

sind.

Nun setze man

$$\left.\begin{array}{ll} \alpha + \alpha^{13} + \alpha^{-1} + \alpha^{-13} = z_1; & \alpha^3 + \alpha^5 + \alpha^{-3} + \alpha^{-5} = z_3 \\ \alpha^9 + \alpha^{15} + \alpha^{-9} + \alpha^{-15} = z_2; & \alpha^{10} + \alpha^{11} + \alpha^{-10} + \alpha^{-11} = z_4 \end{array}\right\}, \quad (6)$$

also

$$z_1 + z_2 = y_1; \; z_3 + z_4 = y_2 \quad \ldots\ldots\ldots\ldots (7)$$

Die Gleichung, deren Wurzeln die 8 in y_1 vorkommenden Wurzeln sind, wird vom 8ten Grade; der eine Coefficient derselben ist $-y_1$, und die übrigen können dann rational durch diesen ausgedrückt werden. Das Product $z_1 z_2$ muss deshalb rational durch y_1 ausgedrückt werden können, da es nicht durch Vertauschung der in y_1 vorkommenden Wurzeln verändert wird. Das Product erhält 16 Glieder, welche alle Wurzeln sind; unter diesen ist α^{10}, welche zu y_2, und α^8,

welche zu y_1 gehört. Die übrigen Glieder von y_1 und y_2 müssen sich deshalb auch unter den 16 Gliedern finden, so dass man erhält

$$z_1 z_2 = y_1 + y_2 = -1,$$

und auf dieselbe Weise, oder indem man α^3 statt α setzt,

$$z_3 z_4 = -1.$$

Diese Grössen sind deshalb Wurzeln der Gleichungen

$$z^2 - y_1 z - 1 = 0 \text{ und } z^2 - y_2 z - 1 = 0. \dots\dots \quad (8)$$

Endlich setze man

$$\alpha + \alpha^{-1} = t_1,$$

$$\alpha^{13} + \alpha^{-13} = t_2,$$

also

$$t_1 + t_2 = z_1;\; t_1 t_2 = z_3.$$

Da t_1 t_2 rational durch z_1 und y_1 muss ausgedrückt werden können, muss dasselbe auch mit z_3 der Fall sein; in Wirklichkeit erhält man auch

$$z_1^2 = z_2 + 2z_3 + 4 \text{ oder } 2z_3 = z_1^2 + z_1 - y_1 - 4;$$

t_1 und t_2 werden also durch die Gleichung

$$t^2 - z_1 t + z_3 = 0 \dots\dots\dots\dots \quad (9)$$

bestimmt.

6 andere Ausdrücke, analog denen für t_1 und t_2, werden auf ähnliche Weise bestimmt; diese 8 Werthe sind eben die Wurzeln der Gleichung 8ten Grades, auf welche die gegebene Gleichung als reciproke Gleichung reducirt werden kann. Diese Werthe sind

$$2 \cos a;\; 2 \cos 2a \dots 2 \cos 8a,$$

wo

$$a = \frac{2\pi}{17}.$$

Da nun für den Radius 1 die Seite des 34ecks

$$2 \sin \frac{\pi}{34} = 2 \cos \frac{8\pi}{17} = 2 \cos 4a,$$

findet sich dieselbe unter diesen Wurzeln; man construirt dieselbe leicht mittelst Zirkel und Lineal mit Hülfe der drei Gleichungen zweiten Grades, indem man zuerst y und z construirt. Dadurch theilt man die Peripherie in 34 gleiche Theile, und durch Ueberschlagen jedes anderen Theilpunktes in 17 gleiche Theile.

Reduction der Gleichung $x^{13} = 1$.

89. Die Methode mag noch auf den Fall angewendet werden, wo $p = 13$; hier hat man $r = 2$ und nach Division durch $x - 1$ die Wurzeln

$$\alpha,\ \alpha^2,\ \alpha^4,\ \alpha^8,\ \alpha^3,\ \alpha^6,\ \alpha^{-1},\ \alpha^{-2},\ \alpha^{-4},\ \alpha^{-8},\ \alpha^{-3},\ \alpha^{-6}.$$

Aus

$$y_1 = \alpha + \alpha^4 + \alpha^3 + \alpha^{-1} + \alpha^{-4} + \alpha^{-3}$$
$$y_2 = \alpha^2 + \alpha^8 + \alpha^6 + \alpha^{-2} + \alpha^{-8} + \alpha^{-6}$$

folgt

$$y_1 + y_2 = -1;\ y_1 y_2 = -3,$$

so dass man erhält

$$y^2 + y - 3 = 0.$$

Man setze nun

$$z_1 = \alpha + \alpha^{-1};\ z_2 = \alpha^4 + \alpha^{-4};\ z_3 = \alpha^3 + \alpha^{-3}$$

also

$$z_1 + z_2 + z_3 = y_1,$$
$$z_1 z_2 + z_1 z_3 + z_2 z_3 = -1.$$
$$z_1 z_2 z_3 = 2 + y_2 = 1 - y_1.$$

Die 6 Werthe von $\cos\frac{2k\pi}{13}$ werden also bestimmt durch die Gleichungen

$$y^2 + y - 3 = 0,$$

$$z^3 - y z^2 - z + y - 1 = 0.$$

Ueber eine Eigenschaft der Function $\frac{x^p - 1}{x - 1}$, wenn p eine Primzahl ist.

90. Die Gleichung

$$X = \frac{x^p - 1}{x - 1} = 0, \ldots\ldots\ldots\ldots \quad (1)$$

wo p eine Primzahl ist, hat die Wurzeln

$$\alpha, \alpha^r, \alpha^{r^2} \ldots \alpha^{r^{p-2}}.$$

Setzt man nun wie oben

$$\left.\begin{aligned} y_1 &= \alpha + \alpha^{r^2} + \alpha^{r^4} \ldots \alpha^{r^{p-3}} \\ y_2 &= \alpha^r + \alpha^{r^3} + \alpha^{r^5} \ldots \alpha^{r^{p-2}} \end{aligned}\right\}, \ldots\ldots\ldots \quad (2)$$

so hat man

$$y_1 + y_2 = -1;$$

p kann nun von der Form $4n + 1$ oder von der Form $4n + 3$ sein.

1) $p = 4n + 1$.

Die conjugirten Wurzeln finden sich in derselben Gruppe, so dass $y_1 y_2$ das Glied 1 nicht enthält. Die Anzahl der

Glieder in $y_1\, y_2$ beträgt $4\,n^2$; unter diesen muss jede Wurzel n Male vorkommen, so dass man erhält

$$y^2 + y - n = 0,$$

woraus

$$y = \frac{-1 \pm \sqrt{p}}{2} \dots\dots\dots\dots\dots \quad (3)$$

Die Gleichung, welche die in y_1 vorkommenden Wurzeln hat, muss Coefficienten von der Form $a + b\,y_1$ haben, wo a und b ganze Zahlen sind. Bildet man nämlich die Summe der Producte von q der Wurzeln, um die Coefficienten der Gleichung zu berechnen, so erhält man eine Summe, wo jedes Glied wiederum eine der Wurzeln ist; die Wurzeln können theils 1 sein, theils Glieder von y_1, theils Glieder von y_2, aber wenn ein Glied von y_1 im Producte vorkommt, müssen sie dort alle sein. Die Summe erhält deshalb die Form $a\,y_1 + b\,y_2 + c$, oder $(a - b)\,y_1 + c - b$, wo a, b und c ganze Zahlen sind und wo man haben muss

$$2\,n\,(a + b) + c = C_q(2\,n),$$

indem beide Zahlen die Anzahl der Glieder in dem berechneten Coefficienten angeben. Vertauscht man α mit α^r, also y_1 mit y_2, erhält man die Gleichung, deren Wurzeln die Glieder von y_2 sind. Werden die Werthe von y_1 und y_2 eingesetzt, unterscheiden sich die beiden Gleichungen nur dadurch von einander, dass $\sqrt{p}$ in ihnen mit entgegengesetztem Vorzeichen vorkommt; andere Nenner als 2 sind nicht vorhanden; deshalb kann man die Gleichungen

$$\frac{Y + \sqrt{p}\,Z}{2} = 0 \text{ und } \frac{Y - \sqrt{p}\,Z}{2} = 0$$

schreiben, wo Y und Z ganze rationale Coefficienten haben; dann hat man identisch

$$4\,X = Y^2 - p\,Z^2.$$

Y ist vom Grade $\frac{p-1}{2}$, Z vom Grade $\frac{p-3}{2}$; da die beiden Gleichungen, welche gebildet werden, reciproke Gleichungen sind, sieht man ferner leicht, dass die Coefficienten von Y und Z eine symmetrische Reihe wie in reciproken Gleichungen bilden.

2) $p = 4n + 3$.

Die in y_1 vorkommenden Wurzeln sind die reciproken Werthe von den in y_2 vorkommenden; unter den $(2n+1)^2$ Gliedern von $y_1 y_2$ findet 1 sich deshalb $2n+1$ Male; jede der übrigen Wurzeln muss dann n Male vorkommen; man erhält deshalb

$$y^2 + y + n + 1 = 0,$$

$$y = \frac{-1 \pm \sqrt{-p}}{2}.$$

Verfährt man wie oben, erhält man also

$$4X = Y^2 + pZ^2.$$

Die beiden Gleichungen sind in diesem wie in dem vorhergehenden Falle nur von einander verschieden durch das Vorzeichen von $\sqrt{-p}$; sie sind nicht wie vorhin reciprok, sondern die eine wird aus der anderen gebildet, wenn x mit $\frac{1}{x}$ vertauscht und die Brüche fortgeschafft werden; mit Hülfe hiervon ergiebt sich leicht, dass die Coefficienten von Z dieselbe Eigenschaft wie oben haben, während die gleich grossen Cofficienten von Y entgegengesetzte Vorzeichen haben.

Die obenstehende Entwicklung gilt nicht für $p = 3$; für diesen Fall hat man

$$4(x^2 + x + 1) = Y^2 + 3Z^2,$$

wo

$$Y = 2x + 1; \; Z = 1$$

oder

$$Y = x + 2;\ Z = x$$

oder

$$Y = x - 1;\ Z = x + 1.$$

Die hier bewiesenen Sätze über die Form des Polynoms X lassen sich mit Vortheil bei der Theorie der ganzen Zahlen benutzen.



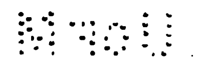
Siebentes Kapitel.

Gleichungen, welche durch Quadratwurzeln aufgelöst werden können.

Form der Wurzeln.

91. x_1 möge eine Wurzel einer gewissen irreductiblen Gleichung sein und durch rationale Grössen und durch Quadratwurzeln ausgedrückt werden können; wenn gesagt wird, dass ein solcher Ausdruck n Quadratwurzeln enthält, so sind n verschiedene gemeint; ein Ausdruck, der nur Quadratwurzeln aus rationalen Grössen enthält, soll ein Ausdruck erster Ordnung heissen; kommen solche Grössen wieder unter dem Quadratwurzelzeichen vor, so ist der Ausdruck von der zweiten Ordnung u. s. w.

Falls unter den in x_1 vorkommenden Wurzelgrössen eine Gleichung mit rationalen Coefficienten existirt, welche mit Rücksicht auf die Wurzelgrössen vom ersten Grade ist, so wird diese benutzt, um eine derselben durch die übrigen auszudrücken und auf die Weise aus dem Ausdruck für x_1 fortzuschaffen. Wenn x_1 auf solche Weise durch eine möglichst geringe Anzahl von Wurzelgrössen ausgedrückt ist, werden die irrationalen Nenner fortgeschafft; dadurch wird keine neue Wurzelgrösse eingeführt, sobald man die Ausführung



der Multiplication in solchen Fällen unterlässt, wo kein Wurzelzeichen dadurch fortgebracht wird. In x_1 kommen nun die Wurzelgrössen, welche nicht wiederum unter einem Wurzelzeichen stehen, nur in der ersten Potenz vor, da das Wurzelzeichen fortfällt, wenn die Wurzelgrösse in einer Potenz mit geradem Exponenten vorkommt. Hieraus folgt zugleich, *dass jede rationale Function der in x_1 vorkommenden Wurzelgrössen mit Beziehung auf diese als ganze rationale Function vom ersten Grade ausgedrückt werden kann.*

Vertauscht man die Vorzeichen der in x_1 vorkommenden Wurzelgrössen auf alle möglichen Arten, so bildet man neue Werthe, welche durch $x_2, x_3 \ldots x_\mu$ bezeichnet werden mögen. Wenn p Wurzelgrössen vorhanden sind, erhält x 2^p Werthe, aber diese sind nicht immer alle verschieden. So wird z. B.

$$\sqrt{a+\sqrt{b}}+\sqrt{a-\sqrt{b}}$$

nicht verändert werden, wenn $\sqrt{b}$ das Vorzeichen wechselt.

Ist x_1 eine Wurzel der irreductiblen Gleichung

$$f(y)=0, \quad \ldots \ldots \ldots \ldots \quad (1)$$

so sind $x_2, x_3 \ldots x_\mu$ es auch.

Man denke sich nämlich x_1 in f(x) eingesetzt, wodurch man einen Ausdruck vom ersten Grade mit Beziehung auf die in x_1 vorkommenden Wurzelgrössen erhält. Da nun keine solche Relation zwischen diesen existirt, muss jede von ihnen den Coefficienten Null erhalten. Die dadurch erhaltenen Gleichungen, welche die Bedingungen dafür ausdrücken, dass x_1 Wurzel ist, können wiederum Wurzelgrössen enthalten; jede derselben lässt sich dann in mehrere andere zerlegen und so fährt man fort, bis man zu einem System von Bedingungsgleichungen gelangt, welche nur rationale Grössen enthalten, nämlich theils solche, welche in f(x) vorkommen, und theils solche, welche durch Quadrirung von Wurzelgrössen in x_1 entstanden sind. Welcher Art diese Bedingungsgleichungen auch sein mögen, sie werden

unabhängig sein von den Vorzeichen der einzelnen Wurzelgrössen und müssen also befriedigt werden durch alle Combinationen dieser Vorzeichen, sobald ihnen durch eine Combination Genüge geleistet wird. Wird also der Gleichung durch x_1 Genüge geleistet, so geschieht dies auch durch $x_2, x_3 \ldots x_\mu$.

Nun kann man

$$x_1 = A + B\sqrt{C}$$

setzen, wo $\sqrt{C}$ eine von den Wurzelgrössen ist, welche nicht wiederum unter einem Wurzelzeichen vorkommt. $\sqrt{C}$ kommt dann nicht in A und B, welche die übrigen Wurzelgrössen enthalten, vor. Setzt man nun

$$x_2 = A - B\sqrt{C},$$

wird das Product

$$(x - x_1)(x - x_2)$$

$\sqrt{C}$ nicht enthalten. Durch Vertauschung der Vorzeichen der in A und B vorkommenden Wurzelgrössen bildet man die analogen Producte für die übrigen Wurzeln und erhält dadurch das Prodnct

$$(x - x_1)(x - x_2) \ldots (x - x_\mu)$$

ausgedrückt als ein Product von 2^{p-1} Factoren zweiten Grades, welche alle aus einem derselben durch Vertauschung der Vorzeichen der Wurzelgrössen gebildet werden. Zwei von diesen Factoren können unter der Form

$$x^2 + (A_1 + B_1\sqrt{C_1})x + A_2 + B_2\sqrt{C_1}$$

und

$$x^2 + (A_1 - B_1\sqrt{C_1})x + A_2 - B_2\sqrt{C_1}$$

dargestellt werden, so dass man, wenn man das Product derselben bildet, einen Factor 4ten Grades erhält, dessen erstes Glied x^4 ist, und der die Wurzelgrösse $\sqrt{C_1}$ nicht enthält;

aus diesem werden dann die analogen Factoren 4ten Grades gebildet. Fährt man auf diese Weise fort, so gelangt man zuletzt zu einer Gleichung vom Grade 2^p mit rationalen Coefficienten und mit den Wurzeln $x_1, x_2 \dots x_\mu$. Falls diese Gleichung irreductibel ist, muss sie die gegebene sein, aber es ist möglich, dass mehrere der Werthe von x unter einander gleich gross werden, so dass die gebildete Gleichung reductibel ist. In diesem Falle muss sie alle Wurzeln von $f(x) = 0$ gleich oft enthalten, denn im entgegengesetzten Falle könnte man durch Division mit einer gewissen Potenz von $f(x)$ eine Gleichung bilden, welche einige der Wurzeln von $f(x) = 0$ enthielte, aber nicht alle. Der Grad der gegebenen Gleichung muss deshalb ein Divisor von 2^p sein. Folglich: *Eine irreductible Gleichung, welche durch Quadratwurzeln aufgelöst werden kann, muss von einem Grade sein, der eine Potenz von 2 ist, und die Wurzeln sind nur verschieden durch die Vorzeichen der sie zusammensetzenden Wurzelgrössen.*

92. *Eine Wurzel einer irreductiblen Gleichung vom Grade 2^p, welche durch Quadratwurzeln aufgelöst werden kann, kann durch p Wurzelgrössen ausgedrückt werden.*

In die Gleichung

$$f(x) = 0 \quad \dots\dots\dots\dots\dots\dots \quad (1)$$

setze man $\frac{k}{x}$ statt x ein, schaffe die Brüche fort und suche auf gewöhnliche Weise die gemeinschaftlichen Wurzeln der beiden Gleichungen. Der Rest vom ersten Grade, zu welchem man bei der Division gelangt, sei

$$Mx + N, \quad \dots\dots\dots\dots\dots\dots \quad (2)$$

während der zuletzt gebrauchte Divisor

$$Ax^2 + Bx + C$$

sein möge, wo M, N, A, B und C ganze rationale Functionen von k und bekannten Grössen bedeuten. Sind nun x_1 und x_2 zwei Wurzeln der Gleichung (1), und setzt man $k = x_1 x_2$,

so müssen x_1 und x_2 gemeinschaftliche Wurzeln der beiden Gleichungen sein, so dass

$$x_1 + x_2 = -\frac{B}{A};\ x_1 x_2 = \frac{C}{A} = k.$$

Die allgemeine Form für einen Factor zweiten Grades, ausgedrückt durch das Product von zwei Wurzeln, ist dann

$$x^2 + \varphi(k)\,x + k,$$

wo φ eine rationale Function ist.

Die beiden Wurzeln werden also, wenn k bekannt ist, durch eine Gleichung zweiten Grades gefunden und werden deshalb durch eine Wurzelgrösse mehr ausgedrückt, als in k vorkommt.

Da die Grösse k ein Product von zweien der Wurzeln ist, wird sie bestimmt durch eine Gleichung vom Grade

$$\frac{2^p(2^p-1)}{2} = 2^{p-1}(2^p-1).$$

Da nun k durch Quadratwurzeln ausgedrückt werden kann, muss die Gleichung in k sich in Gleichungen zerlegen lassen, deren Grade Potenzen von 2 sind; diese können nicht alle vom Grade 2^p oder von einem höheren Grade sein, denn eine Summe von solchen Potenzen von 2 ist theilbar durch 2^p, während der Grad der Gleichung in k nicht theilbar ist durch 2^p. Der Grad von wenigstens einer der Gleichungen kann deshalb nicht über 2^{p-1} hinausgehen. Die Gleichung vom Grade 2^p kann deshalb durch p Wurzelgrössen aufgelöst werden, sobald eine Gleichung vom Grade 2^{p-1} durch $p-1$ Wurzelgrössen aufgelösst werden kann. Da nun die Gleichung zweiten Grades durch eine Wurzelgrösse aufgelöst werden kann, ist der Satz bewiesen. Indessen giebt es einen Fall, welcher genauer untersucht werden muss, nämlich den, wo der gemeinschaftliche Factor von $f(x)$ und $f\left(\frac{k}{x}\right)$ von höherem als dem zweiten Grade wird. Das kann nur eintreten, wenn

$$x_p = \frac{k}{x_q}$$

durch andere Werthe von p und q als 1 und 2 befriedigt wird; dann hätte man

$$x_p x_q = x_1 x_2,$$

oder, wenn man $x + h$ statt x setzt,

$$x_p x_q + h(x_p + x_q) + h^2 = x_1 x_2 + h(x_1 + x_2) + h^2;$$

dies kann nicht für alle Werthe von h gelten, es sei denn dass die gegebene Gleichung gleiche Wurzeln habe, was, weil sie irreductibel, nicht der Fall sein kann. In dem Falle, wo der geführte Beweis ungültig wird, kann man deshalb immer die Gleichung so transformiren, dass der Beweis seine Gültigkeit behält. Da diese Transformation die Anzahl der in x vorkommenden Wurzelgrössen aber nicht verändert, gilt der Satz immer.

93. Werden nun wie oben die Factoren

$$x - x_1, \; x - x_2, \ldots x - x_\mu$$

paarweise zusammengezogen, die neuen Factoren zweiten Grades wiederum paarweise u. s. w., so wird jedesmal eine Wurzelgrösse fortgeschafft; wenn nur eine Wurzelgrösse $\sqrt{\alpha}$ übrig ist, erhält man zwei Factoren, welche sich nur durch das Vorzeichen von $\sqrt{\alpha}$ unterscheiden; die Gleichung vom Grade 2^p kann deshalb auf eine Gleichung vom Grade 2^{p-1} reducirt werden, in der $\sqrt{\alpha}$ in den Coefficienten vorkommt. Vereinigt man die Glieder, welche $\sqrt{\alpha}$ als Factor enthalten, erhält die Gleichung die Form

$$x^m + a_1 x^{m-1} + a_2 x^{m-2} \ldots + a_m \pm \sqrt{\alpha}\left(b_1 x^{m-1} + b_2 x^{m-2} + \ldots b_m\right) = 0,$$

worin $m = 2^{p-1}$; man kann immer dafür Sorge tragen, dass der Coefficient der höchsten Potenz von x 1 ist, ohne dass $\sqrt{\alpha}$ in den Nennern der Coefficienten vorkommt.

Ist die gegebene Gleichung

$$f(x) = 0,$$

muss man also haben

$$f(x) = \left(x^m + a_1 x^{m-1} + \ldots + a_m\right)^2 - \alpha\left(b_1 x^{m-1} + b_2 x^{m-2} + \ldots + b_m\right)^2;$$

$\sqrt{\alpha}$ ist hier die Wurzelgrösse, welche zuletzt aus x_1 fortgeschafft wird, das heisst diejenige, welche man erst berechnen muss, wenn man den Werth von x_1 berechnen will. Hat man die Wahl zwischen mehreren, kann $f(x)$ auf ebenso viele Arten auf die angegebene Form gebracht werden; hat man z. B.

$$x_1 = \sqrt{a} + \sqrt{b} + \sqrt{\sqrt{a} + \sqrt{b}} + k,$$

wird $f(x)$ auf die beiden Formen

$$A^2 - a B^2 \text{ und } A^2 - b B^2$$

gebracht werden können, wo A vom vierten, B vom dritten Grade ist.

Auflösung der Gleichung.

94. Um die gegebene Gleichung zu reduciren, kann man die Gleichung bilden, deren Wurzeln durch alle Werthe von

$$(x_1 + x_2 + \cdots + x_m)(x_{m+1} + x_{m+2} + \cdots + x_{2m})$$

dargestellt werden.

Der Grad g dieser Gleichung ist gleich der halben Anzahl von Arten, auf welche man 2^{p-1} Grössen aus 2^p Grössen entnehmen kann, oder

$$g = \frac{2^p!}{2(2^{p-1}!)^2}.$$

Man kann beweisen, dass diese Zahl ungerade ist; wenn man nämlich alle geraden Factoren von $2^p!$ durch 2 dividirt,

erhält man alle Factoren von $2^{p-1}!$; man erhält deshalb, wenn u, u_1, u_2 ungerade Zahlen bezeichnen

$$2^p! = 2^{2^{p-1}} . 2^{p-1}! \, u.$$

Setzt man hierin nach und nach $p-1, p-2, \ldots 1$ statt p ein, und multiplicirt die erhaltenen Gleichungen, so folgt

$$2^p! = 2^{2^p - 1} u \, u_1 \, u_2 \ldots,$$

während man für den Nenner von g erhält

$$2^{2^p - 1} u_1^2 \, u_2^2 \ldots,$$

also

$$g = \frac{u}{u_1 \, u_2 \ldots},$$

mithin eine ungerade Zahl.

Da nun die so gebildete Gleichung mittelst Quadratwurzeln aufgelöst werden kann, wenn dieses mit der gegebenen der Fall ist, so muss sie in Gleichungen zerlegt werden können, deren Grade Potenzen von 2 sind; da der Grad ungerade ist, muss deshalb eine von diesen Gleichungen vom ersten Grade sein, so dass unter den Werthen des Productes einer sein muss, welcher rational ist. Dieser kann durch Versuche gefunden werden, wenn die Hülfsgleichung gebildet ist, da er ein Factor des letzten Gliedes dieser Gleichung sein muss. Da man nun ausserdem die Summe der beiden Factoren des Productes kennt, werden diese durch eine Gleichung zweiten Grades mit rationalen Coefficienten bestimmt. Man kennt nun die Summe der m Wurzeln, ausgedrückt durch eine Quadratwurzel, und die übrigen symmetrischen Functionen dieser m Wurzeln können dann als rationale Functionen der gefundenen Summe und bekannter Grössen dargestellt werden. Die Gleichung, welche diese m Wurzeln bestimmt, erhält deshalb die Form

$$x^m + (a_1 + b_1 \sqrt{\alpha}) \, x^{m-1} + (a_2 + b_2 \sqrt{\alpha}) \, x^{m-2} + \ldots a_m + b_m \sqrt{\alpha} = 0,$$

wo a_1, b_1, $a_2 \ldots a_m$, b_m und α rational sind. Vertauscht

man $+\sqrt{\alpha}$ mit $-\sqrt{\alpha}$, so erhält man die Gleichung, welche die übrigen m Wurzeln bestimmt.

Behandelt man die reducirte Gleichung auf dieselbe Weise, wie die gegebene behandelt wurde, indem man $\sqrt{\alpha}$ als eine bekannte Grösse behandelt, so erhält man eine Gleichung vom Grade 2^{p-2}, deren Coefficienten rationale Functionen von $\sqrt{\alpha}$ und einer neuen Quadratwurzel sind. Hier bietet sich indessen die Schwierigkeit, dass die als rational betrachtete Wurzel der Hülfsgleichung, welche gefunden werden soll, von der Form $b + c\sqrt{\alpha}$ wird und als Factor eines Ausdrucks von derselben Form, nämlich des letzten Gliedes der Gleichung, gesucht werden muss. Doch kann man durch Vertauschung von x mit $y + z\sqrt{\alpha}$ die Gleichung in zwei andere zerlegen, in denen die rationalen Grössen b und c Wurzeln werden.

Eine Bedingung für die Möglichkeit der Auflösung.

95. Während es auf diese Weise immer möglich ist, eine Gleichung aufzulösen, welche durch Quadratwurzeln aufgelöst werden kann, wird die praktische Ausführung bereits für Gleichungen 8ten Grades sehr beschwerlich werden. Man kann in der Praxis oft mit Vortheil folgenden Satz benutzen:

Falls die Gleichung $f(x) = 0$ auf den halben Grad reducirt werden kann, muss man, wenn man auf gewöhnliche Weise die Quadratwurzel aus $f(x)$ zieht, zu einem Rest gelangen, welcher theilbar ist durch α, wenn $\sqrt{\alpha}$ die Quadratwurzel ist, welche bei der Reduction eingeführt wird.

Angenommen, die Gleichung sei

$$x^{2m} + A_1 x^{2m-1} \ldots + A_m = 0 \quad \ldots\ldots\ldots\ldots \quad (1)$$

und könne auf die Form

$$\left(x^m + a_1 x^{m-1} + \ldots + a_m\right)^2 - \alpha\left(b_1 x^{m-1} + b_2 x^{m-2} + \ldots b_m\right)^2 = 0. \quad (2)$$

gebracht werden, während sie durch Ausziehen der Quadratwurzel die Form

$$\left(x^m + k_1 x^{m-1} + k_2 x^{m-2} + \ldots k_m\right)^2 + R_{m-1} = 0 \;\ldots\ldots\; (3)$$

annimmt, wo R_{m-1} höchstens vom Grade $m-1$ ist. Dann muss man identisch haben

$$\left(2x^m + (a_1 + k_1)x^{m-1} + (a_2 + k_2)x^{m-2} + \ldots a_m + k_m\right)\left((a_1 - k_1)x^{m-1} + (a_2 - k_2)x^{m-2} \ldots + a_m - k_m\right) = \alpha\left(b_1 x^{m-1} + b_2 x^{m-2} + \ldots + b_m\right)^2 + R_{m-1}. \;\ldots\ldots\; (4)$$

Durch Vergleichung der Coefficienten von

$$x^{2m-1},\; x^{2m-2} \ldots x^m,$$

wo also der Rest ohne Einfluss bleibt, erhält man

$$\left.\begin{array}{l} 2(a_1 - k_1) = 0 \\ 2(a_2 - k_2) + (a_1 + k_1)(a_1 - k_1) = \alpha b_1^2 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ 2(a_p - k_p) + (a_1 + k_1)(a_{p-1} - k_{p-1}) + \ldots = \alpha A \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ 2(a_m - k_m) + (a_1 + k_1)(a_{m-1} - k_{m-1}) \\ \qquad + \ldots (a_{m-1} + k_{m-1})(a_1 - k_1) = \alpha B, \end{array}\right\} \;\ldots\; (5)$$

worin αA und αB Grössen bedeuten, die durch α theilbar sind.

Die erste dieser Gleichungen zeigt, dass $a_1 = k_1$; die zweite, dass $a_2 - k_2$, wenn man vom Factor 2 absieht, theilbar ist durch α, die folgende, dass $a_3 - k_3$ theilbar ist durch α und so fort, bis die letzte zeigt, dass $a_m - k_m$ theilbar ist durch α. α wird also ein Factor der linken Seite der Identität (4) und muss deshalb auch ein Factor von R_{m-1} sein.

Wenn die Wurzel mehrere Quadratwurzeln erster Ordnung hat, kann jede von diesen wie $\sqrt{\alpha}$ behandelt werden,

und alle Factoren der rationalen Grössen α müssen sich deshalb in allen Gliedern von R_{m-1} finden.

Beispielsweise soll die Gleichung betrachtet werden, auf welche $x^{17} - 1 = 0$ reducirt werden kann, nämlich

$$f(x) = x^8 + x^7 - 7x^6 - 6x^5 + 15x^4 + 10x^3 - 10x^2 - 4x + 1 = 0.$$

Durch Ausziehen der Quadratwurzel erhält man

$$2^{12} R_{m-1} = -17 . 32 x^3 - 17 . 88 x^2 - 17 . 92 x - 17 . 1273.$$

Die Gleichung kann in Wirklichkeit auch folgendermassen ausgedrückt werden:

$$x^4 + \frac{1}{2} x^3 - \frac{3}{2} x^2 + 2x - 1 = \pm \frac{\sqrt{17}}{2} (x^3 + x^2 - 2x).$$

Anwendung auf ein geometrisches Problem.

96. Gleichungen, welche durch Quadratwurzeln aufgelöst werden können, haben eine besondere Bedeutung für die Geometrie, da jedes Problem, welches mit Hülfe von Zirkel und Lineal gelöst werden kann, auf solche Gleichungen führen muss. Jede Construction ist nämlich zusammengesetzt aus den beiden elementaren, eine gerade Linie durch zwei gegebene Punkte zu ziehen und einen Kreis mit gegebenem Mittelpunkt und gegebenem Radius zu zeichnen. Wenn man nach und nach diese Constructionen ausführt, kann man mittelst der Formeln der analytischen Geometrie die gefundenen Stücke durch die gegebenen ausdrücken; da man hierbei nicht dazu kommt, Gleichungen von höherem als dem zweiten Grade aufzulösen, *müssen die gesuchten Grössen sich durch die gegebenen immer mittelst Quadratwurzeln ausdrücken lassen.*

Hieraus folgt dann die Unmöglichkeit der Dreitheilung des Winkels mittelst Zirkel und Lineal; man kann nämlich den cos. des gesuchten Winkels als die zu construirende

Grösse nehmen; da dieser indessen durch eine irreductible Gleichung dritten Grades bestimmt wird, kann derselbe nicht durch Quadratwurzeln ausgedrückt werden.

Die meisten Constructionsaufgaben lassen sich zurückführen auf die Bestimmung eines Punktes, der wiederum durch zwei geometrische Oerter bestimmt wird. Falls der eine von diesen eine gerade Linie in einer ganz willkürlichen Lage und der andere eine davon unabhängige Curve ist, kann man die Ordnung dieser Curve bestimmen, sobald die Aufgabe sich mit Zirkel und Lineal lösen lassen soll. Weniger allgemein kann man suchen die Curve zu bestimmen, sobald die gerade Linie nur einen willkürlichen Parameter hat, und namentlich wenn sie durch einen gegebenen Punkt gehen soll.

97. Es sei also ein Strahlenbüschel gegeben, dessen Scheitel zum Anfangspunkt des Coordinatensystems genommen werde. *Dann würde die Aufgabe darin bestehen, alle die Curven zu finden, deren Durchschnittspunkte mit einer beliebigen Linie des Büschels mit Hülfe von Zirkel und Lineal bestimmt werden können.* Es werde angenommen, dass die Curve nicht durch den Anfangspunkt gehe; nun führe man Polarcoordinaten ein, indem man

$$x = m r; \; y = n r \quad \ldots\ldots\ldots\ldots\ldots \quad (1)$$

setzt; die Gleichung der Curve nimmt dann die Form

$$a + b r + c r^2 + \ldots = 0 \quad \ldots\ldots\ldots\ldots \quad (2)$$

an, worin a nicht Null sein kann, und wo a, b, c ... homogene Functionen von m und n von den Graden 0, 1, 2 u. s. w. sind.

Wenn die Aufgabe mit Zirkel und Lineal lösbar sein soll, muss sich diese Gleichung für jedes m und n auflösen lassen können. Es existirt ganz sicher zwischen m und n eine Relation, so dass nur das Verhältniss derselben willkürlich ist, aber man kann immer km und kn für m und n einsetzen, wenn man gleichzeitig r in $\frac{r}{k}$ verändert; deshalb

kann man m und n als von einander unabhängig betrachten. Zufolge des Gegebenen sind die Constanten der Curve von m und n unabhängig. Man sieht leicht, dass die Gleichuug irreductibel ist, sobald die Curve nicht zusammengesetzt ist.

Soll die Gleichung (2) durch Quadratwurzeln aufgelöst werden können, so muss sie, wenn k und k_1 ganze Functionen sind, auf die Form

$$k(A + Br + Cr^2 \ldots)^2 = k_1 (A_1 + B_1 r + C_1 r^2 \ldots)^2 \quad \ldots \quad (3)$$

gebracht werden können; diese kann übrigens erst als identisch mit (2) gedacht werden, nachdem ein Factor durch Division entfernt worden ist. Durch Vergleichuug der Gleichungen sieht man, dass dieser

$$\frac{k A^2 - k_1 A_1^2}{a}$$

ist, oder nur

$$\varphi = k A^2 - k_1 A_1^2,$$

da a unabhängig von m und n ist und deshalb durch Division entfernt werden kann, ohne dass die Form der Gleichung verändert wird. Man kann annehmen, dass k und k_1 keinen gemeinschaftlichen Factor haben, da dieser durch Division zum Wegfall gebracht werden kann; ferner, dass φ keinen Factor mit k oder k_1 gemeinschaftlich hat, da ein Factor, der φ und k_1 gemeinsam ist, auch ein Factor von A, B, C ... sein müsste, so dass er fortdividirt werden könnte, ohne dass die Form der Gleichung verändert würde.

Man kann nun (3) unter der Form

$$[A\sqrt{k} + A_1\sqrt{k_1} + (B\sqrt{k} + B_1\sqrt{k_1})r + \ldots] \\ [A\sqrt{k} - A_1\sqrt{k_1} + (B\sqrt{k} - B_1\sqrt{k_1})r + \ldots] = 0$$

darstellen; multiplicirt man den ersten Factor mit $A\sqrt{k} - A_1\sqrt{k_1}$, den zweiten mit $A\sqrt{k} + A_1\sqrt{k_1}$, so erhält man die Form

$$[\varphi + (M + N\sqrt{kk_1})r + (M_1 + N_1\sqrt{kk_1})r^2 + \ldots] \\ [\varphi + (M - N\sqrt{kk_1})r + (M_1 - N_1\sqrt{kk_1})r^2 + \ldots] = 0,$$

wo die linke Seite theilbar sein muss durch φ^2.

Man kann hier zeigen, dass jeder der beiden Factoren theilbar sein muss durch φ, denn vertauscht man $+\sqrt{kk_1}$ mit $-\sqrt{kk_1}$, so werden die beiden Factoren vertauscht, während φ unverändert bleibt; es kann deshalb in dem einen Factor keine anderen Factoren von φ^2 geben als in dem anderen. Dividirt man nun beide Factoren durch φ, so erhält man nach Ausführung der Multiplication die obige Gleichung (3), aus der der Factor φ entfernt ist, ohne dass die Form verändert wäre; man kann deshalb annehmen, dass (2) und (3) identisch sind; dann hat man $k A^2 - k_1 A_1{}^2 = a$, unabhängig von m und n; a ist nicht Null, und k uud k_1 können nicht beide constant sein (die Gleichung würde dadurch reductibel werden); die Coefficienten müssen homogene Functionen von m und n sein, da die Gleichung bei der oben angegebenen Substitution unverändert bleiben soll und die Form (3) nur auf eine endliche Anzahl Arten annehmen kann; wenn nun k_1 m und n enthält, muss A_1 Null sein und k und A constant.

Setzt man nun in (3) $k_1 = 0$, so bestimmt man dadurch die Werthe von m und n, für welche alle Durchschnittspunkte der geraden Linie und der Curve zu je zweien zusammenfallen. *Die Curve muss deshalb eine solche Curve der Ordnung 2^p sein, dass sich vom Scheitel des Strahlenbüschels Linien ziehen lassen, von deren Durchschnittspunkten mit der Curve je zwei zusammenfallen.* Da nun $A_1 = 0$, muss k_1 wenigstens vom zweiten Grade mit Beziehung auf m und n sein; also muss der Scheitel des Strahlenbüschels der Durchschnittspunkt von zwei solchen Linien sein. Wenn der Scheitelpunkt auch beliebig ist, wird die Aufgabe nur möglich sein, sobald es nur zwei Durchschnittspunkte giebt.

Ausser den Kegelschnitten giebt es deshalb keine Curven, deren Durchschnittspunkte mit einer beliebigen geraden Linie durch Zirkel und Lineal bestimmt werden können.

Durch Anwendung des Dualitätsprincips folgt hieraus ferner:

Ausser den Kegelschnitten giebt es keine Curven, an welche man mit Hülfe von Zirkel und Lineal Tangenten von einem beliebigen Punkte ziehen kann.

Durchschnitt eines Strahlenbüschels mit Curven vierter Ordnung.

98. Es sollen nun im Besonderen Curven vierter Ordnung betrachtet werden; die Gleichung derselben muss die Form

$$(A + Br + Cr^2)^2 = kr^2 (Dr + E)^2 \quad \ldots\ldots\ldots \quad (1)$$

haben.

Falls E nicht Null ist, muss k vom zweiten Grade sein; ist $E = 0$, kann k als vom vierten Grade betrachtet werden; dadurch gelangt man im ersten Falle zu einer Gleichung von der Form

$$S^2 = \lambda \alpha \beta \gamma^2, \quad \ldots\ldots\ldots\ldots \quad (2)$$

wo $S = 0$ ein beliebiger Kegelschnitt ist, $\gamma = 0$ eine beliebige gerade Linie, λ eine Constante, während $\alpha = 0$ und $\beta = 0$ zwei von den Geraden des Strahlenbüschels sind.

Im zweiten Falle erhält man

$$S^2 = \lambda \alpha \beta \gamma \delta, \ldots\ldots\ldots\ldots \quad (3)$$

wo $\alpha = 0$, $\beta = 0$, $\gamma = 0$ und $\delta = 0$ beliebige Geraden des Büschels sind.

Die erste Gleichung gehört zu einer Curve vierter Ordnung mit zwei Doppelpunkten, die durch $S = 0$ und $\gamma = 0$ bestimmt werden, und mit den Doppeltangenten $\alpha = 0$ und $\beta = 0$, welche sich in dem gegebenen Punkte schneiden, und deren Berührungspunkte, zugleich mit den beiden Doppelpunkten, auf dem Kegelschnitt S liegen.

Die zweite Gleichung gehört zu einer Curve vierter

Ordnung mit vier Doppeltangenten, welche sich in dem gegebenen Punkte schneiden, und deren 8 Berührungspunkte auf S liegen.

Es soll nicht genauer auf den Fall eingegangen werden, wo der gegebene Punkt auf der Curve liegt und dort q fach ist, in welchem Falle die Ordnung der gesuchten Curven um q höher wird. Dagegen soll gezeigt werden, wie man bei der ersten Classe von Curven die gesuchten Durchschnittspunkte mit Hülfe von zwei Kegelschnitten finden kann.

Die Gleichung (1) kann geschrieben werden

$$(C - D\sqrt{k})\,r^2 + (B - E\sqrt{k})\,r + A = 0.$$

Setzt man hier, wenn die Wurzeln r_1 und r_2 sind,

$$\frac{2}{\rho_1} = \frac{1}{r_1} + \frac{1}{r_2},$$

und vertauscht darauf $\sqrt{k}$ mit $-\sqrt{k}$, ρ_1 mit ρ_2, erhält man ρ_1 und ρ_2 bestimmt durch die Gleichung

$$(B^2 - k\,E^2)\,\rho^2 + 4\,AB\rho + 4A^2 = 0,$$

welche einem Kegelschnitt angehört, der für $E = 0$ übergeht in eine Doppellinie,

$$B\rho + 2A = 0,$$

welche Polare ist für den Anfangspunkt mit Beziehung auf S.

Ist E nicht Null, stimmen ρ_1 uud ρ_2 überein für $k = 0$, so dass die Doppeltangenten Tangenten des Hülfskegelschnitts sind.

Da die beiden Durchschnittspunkte mit dem Kegelschnitt nicht für die Bestimmung der vier gesuchten Durchschnittspunkte genügen, bilde man noch einen Hülfskegelschnitt; man kann hier den benutzen, welchen man erhält, wenn man auf jedem Strahl des Büschels die beiden Punkte nimmt, welche sowohl mit r_1 und r_2, als auch mit den beiden anderen

Durchschnittspunkten r_3 und r_4 harmonisch verbunden sind; diese werden bestimmt durch die Gleichungen

$$2(x_1 x_2 + r_1 r_2) = (x_1 + x_2)(r_1 + r_2)$$

$$2(x_1 x_2 + r_3 r_4) = (x_1 + x_2)(r_3 + r_4),$$

wodurch sich als Gleichung für den gesuchten Kegelschnitt ergiebt

$$(BD - CE)x^2 + 2ADx + AE = 0;$$

für $E = 0$ zerfällt dieser in die früher gefundene Linie und eine Linie durch den gegebenen Punkt. In diesem Falle kann die Reduction deshalb nicht angewendet werden, während man, wenn E nicht Null ist, leicht die vier Durchschnittspunkte bestimmt, sobald die Durchschnittspunkte mit den beiden Hülfskegelschnitten erst gefunden sind.

Umgekehrt kann man zwei beliebige Kegelschnitte nehmen und mit Hülfe dieser eine Curve vierter Ordnung von der untersuchten Art construiren. Von einer genaueren Erörterung der Frage wird hier abgesehen und auf eine Abhandlung des Verfassers in Zeuthen's *Tidsskrift, 3. Reihe, 4. Jahrgang,* verwiesen.

DRITTER ABSCHNITT.

UEBER DIE NUMERISCHE AUFLOESUNG DER GLEICHUNGEN.

Erstes Kapitel.

Absonderung der Wurzeln.

Grenzen der reellen Wurzeln.

99. Die algebraische Auflösung der Gleichungen von höherem als dem vierten Grade ist, wie gezeigt worden, nur in ganz besonderen Fällen möglich; hat man eine Gleichung, deren Coefficienten in Zahlen gegeben sind, so kann man indessen, ohne die algebraische Form der Wurzeln zu kennen, die numerischen Werthe derselben mit so grosser Genauigkeit bestimmen, wie man will. Um diese approximative Bestimmung auszuführen, muss man zuerst die Wurzeln *abgesondert* haben, das heisst, man muss für jede Wurzel zwei Zahlen bestimmen, zwischen welchen diese und keine andere Wurzel belegen ist; sind mehrfache Wurzeln vorhanden, so muss man ausserdem angeben, wie oft jede einzelne von diesen vorkommt. Diese Absonderung wird erleichtert, wenn man zuerst *die Grenzen der Wurzeln* bestimmt, das heisst zwei Zahlen, zwischen welchen alle reellen Wurzeln liegen. Hierfür hat man verschiedene Methoden, welche indessen alle nur eine sehr unsichere Annäherung gewähren.

100. *Erste Methode.* Die Gleichung sei

$$x^n + a_1 x^{n-1} \ldots - a_m x^{n-m} \ldots - a_p x^{n-p} \ldots \pm a_n = 0,$$

worin $-a_m$ der erste und $-a_p$ der numerisch grösste negative Coefficient ist; für $x > 1$ muss man dann haben

$$x^n < a_p (x^{n-m} + x^{n-m-1} \ldots + 1) = a_p \frac{x^{n-m+1} - 1}{x - 1},$$

also auch

$$x^n < a_p \frac{x^{n-m+1}}{x-1},$$

woraus folgt

$$x^{m-1}(x-1) < a_p$$

oder

$$x < 1 + \sqrt[m]{a_p} \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Auf die Weise ist eine obere Grenze für die positiven Wurzeln bestimmt.

Diese Grenze kann auf folgende Weise niedriger werden: Man setze

$$x = \frac{y}{\alpha},$$

und wende die gefundene Formel an, um eine obere Grenze für y zu bestimmen; dadurch erhält man

$$y < 1 + \sqrt[m]{a_p \alpha^p}$$

also

$$x < \frac{1}{\alpha} + \sqrt[m]{a_p \alpha^{p-m}} \ldots\ldots\ldots\ldots\ldots (2)$$

Da α eine beliebige positive Grösse ist, kann man den Werth von α wählen, durch welchen die gefundene Grenze so niedrig wie möglich wird; dieser Werth wird bestimmt durch

$$\frac{1}{\alpha^2} = \frac{p-m}{m} \sqrt[m]{a_p}\, \alpha^{\frac{p}{m}-2}$$

oder

$$\alpha^{\frac{p}{m}} = \frac{m}{p-m} a_p^{-\frac{1}{m}},$$

woraus

$$x < \frac{p}{p-m}\left(\frac{p-m}{m}\right)^{\frac{m}{p}} \sqrt[p]{a_p} = p\sqrt[p]{\frac{a_p}{m^m (p-m)^{p-m}}}, \quad . . (3)$$

ein Werth, der für $p = m$ nicht brauchbar ist; für diesen Fall giebt indessen (2) für $\alpha = \infty$

$$x < \sqrt[m]{a_m} \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; (4)$$

Man kann hier nicht für a_p den grössten negativen Coefficienten der gegebenen Gleichung nehmen, da dieser nicht nothwendig den grössten Coefficienten der Gleichung in y giebt; man muss deshalb die höchste Grenze nehmen, welche man erhält, wenn man nach und nach für a_p alle negativen Coefficienten nimmt.

Beisp.

$$x^8 - x^7 + 5x^6 - 15x^5 - 47x^4 + x^3 - 711x^2 - 313x + 1 = 0.$$

Die Grenzwerthe werden

$$1,\ 3\sqrt[3]{\frac{15}{4}},\ 4\sqrt[4]{\frac{47}{27}},\ 6\sqrt[6]{\frac{711}{5^5}},\ 7\sqrt[7]{\frac{313}{6^6}},$$

woraus hervorgeht, dass 5 eine obere Grenze für die positiven Wurzeln ist. Die niedrigste obere Grenze in ganzen Zahlen ist in Wirklichkeit 4.

Vertauscht man x mit $-x$ und sucht die obere Grenze für die positiven Wurzeln der so gebildeten Gleichung, wird diese mit entgegesetztem Vorzeichen eine untere Grenze für die negativen Wurzeln der gegebenen Gleichung sein; hierdurch erhält man den Grenzwerth

$$3\sqrt[6]{\frac{711}{16}} < 6,$$

so dass alle reellen Wurzeln der gegebenen Gleichung zwischen -6 und 5 liegen.

Falls man x mit $\frac{1}{x}$ vertauscht und mittelst der angegebenen Methode findet, dass $\frac{1}{x}$ zwischen zwei Grenzen $-k$ und k_1 liegt, kann x nicht zwischen den Grenzen $-\frac{1}{k}$ und $\frac{1}{k_1}$ belegen sein, so dass die erstere von diesen eine obere Grenze für die negativen, die zweite eine untere Grenze für die positiven Wurzeln der gegebenen Gleichung wird.

101. *Zweite Methode.* Man bringe die Gleichung auf die Form

$$f(x) = \varphi(x) - \varphi_1(x) + \varphi_2(x) = 0,$$

wo $\varphi(x)$ alle Glieder enthält, welche dem ersten Gliede mit negativen Coefficienten vorangehen, $\varphi_2(x)$ die übrigen Glieder mit positiven Coefficienten, während $-\varphi_1(x)$ alle Glieder mit negativen Coefficienten enthält. In die Differenz

$$\varphi(x) - \varphi_1(x)$$

setze man nach und nach grössere und grössere Werthe für x ein, bis man zu einem Werthe k gelangt, welcher dieselbe positiv macht. k ist dann eine obere Grenze für die positiven Wurzeln. Wenn nämlich x^m die niedrigste Potenz von x in $\varphi(x)$ ist, kann die Differenz

$$x^m\left(\frac{\varphi(x)}{x^m} - \frac{\varphi_1(x)}{x^m}\right)$$

geschrieben werden.

Da nun $\frac{\varphi(x)}{x^m}$ lauter positive Coefficienten und positive Exponenten hat, wird der Werth dieses Bruches mit x wachsen, während $\frac{\varphi_1(x)}{x^m}$, worin x lauter negative Exponenten hat, abnehmen wird, wenn x wächst. Ein Werth von x,

welcher grösser ist als k, wird deshalb die Grösse in der Klammer und also auch f (x) positiv machen; da solchergestalt kein Werth grösser als k Wurzel der Gleichung sein kann, ist k die obere Grenze der Wurzeln.

Beisp. Wird in dem oben angeführten Beispiel x mit — x vertauscht, so wird die Gleichung

$$x^8 + x^7 + 5x^6 + 15x^5 - 47x^4 - x^3 - 711x^2 + 313x + 1 = 0.$$

Untersucht man, nach Division durch x^2, den Ausdruck

$$x^6 + x^5 + 5x^4 + 15x^3 - (47x^2 + x + 711),$$

so findet man, dass derselbe positiv wird für $x = 3$. Während oben — 6 als untere Grenze der Wurzeln gefunden wurde, giebt diese Methode also — 3.

Die Methode kann erweitert werden, indem man f (x) in mehrere Gruppen von der Form

$$\varphi(x) - \varphi_1(x)$$

zerlegt, so dass alle Coefficienten in $\varphi(x)$ und $\varphi_1(x)$ positiv sind, während $\varphi_1(x)$ nur Glieder von niedrigerem Grade als die Glieder in $\varphi(x)$ enthält; ein Werth von x, welcher alle Differenzen positiv macht, ist dann eine obere Grenze der Wurzeln.

102. *Newton's Methode. Wenn man in die Polynome*

$$f(x),\ f'(x),\ f''(x) \ldots f^{(n)}(x)$$

nach und nach höhere und höhere Werthe von x einsetzt, bis man zu einem Werthe k gelangt, welcher alle Functionen positiv macht, wird k eine obere Grenze der Wurzeln sein.

Man hat nämlich

$$f(k + h) = f(k) + f'(k)\frac{h}{1} + f''(k)\frac{h^2}{1.2} + \cdots + h^n,$$

woraus hervorgeht, dass

$$f(k + h)$$

immer positiv ist, wenn h positiv und k auf die angegebene Weise bestimmt ist. $k + h$ kann deshalb nicht Wurzel von $f(x) = 0$ sein für irgend welchen positiven Werth von h, und k ist deshalb eine obere Grenze der Wurzeln.

Diese Methode ist mühsamer als die vorhergehenden, giebt aber auch in der Regel engere Grenzen. Die gefundene Grenze kann indessen auch viel zu hoch sein, da sie offenbar nicht allein obere Grenze ist für die Wurzeln von $f(x) = 0$, sondern auch für die von $f'(x) = 0$, $f''(x) = 0$ u. s. w., und diese Gleichungen können Wurzeln haben, welche um ein ganz Beliebiges grösser sind, als die Wurzeln von $f(x) = 0$.

Einige Erleichterungen bei der praktischen Anwendung lassen sich am besten an einem Beispiel zeigen.

Beisp.

$$x^5 + 5x^4 - 10x^3 + x^2 - 16x - 7 = 0.$$

	$x = 0$	1	2	3
$f(x) = x^5 + 5x^4 - 10x^3 + x^2 - 16x - 7$			$-$	$+$
$f'(x) = 5x^4 + 20x^3 - 30x^2 + 2x - 16$		$-$	$+$	
$\frac{1}{2} f''(x) = 10x^3 + 30x^2 - 30x + 1$		$+$		
$\frac{1}{2.3} f'''(x) = 10x^2 + 20x - 10$	$-$	$+$		
$\frac{1}{2.3.4} f^{IV}(x) = 5x + 5$	$+$			
$f^{V}(x)$ $+$				

Man beginnt von unten; $x = 0$ macht $f^{IV}(x)$ positiv, und da dasselbe auch für ein grösseres x gelten muss, ist man fertig mit $f^{IV}(x)$; $x = 1$ macht $f'''(x)$ und $f''(x)$ positiv, aber $f'(x)$ negativ; für $x = 2$ wird darauf $f'(x)$ positiv und $f(x)$ negativ, und da endlich $f(x)$ für $x = 3$ positiv wird, ist 3 eine obere Grenze.

Anzahl der reellen Wurzeln, welche zwischen zwei gegebenen Zahlen belegen sind.

103. Die reellen Wurzeln von $f(x) = 0$, geordnet nach der Grösse, die kleinste voran, seien α_1, α_2, $\alpha_3 \ldots$; dann hat man

$$f(x) = X(x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \ldots,$$

wo X die complexen Wurzeln bestimmt und also nicht für irgend welchen reellen Werth von x gleich Null werden kann. Setzt man nun für x einen Werth ein, der kleiner als α_1 ist, und lässt man diesen Werth wachsen, bis er grösser als die grösste Wurzel geworden ist, wird jedesmal, wenn man eine der Wurzeln passirt, einer der Factoren und folglich auch das Product das Vorzeichen wechseln. f(x) muss deshalb für zwei Werthe von x, zwischen denen eine gerade Anzahl von Wurzeln (oder keine Wurzel) liegt, dasselbe Vorzeichen erhalten, während die beiden Werthe Resultate mit verschiedenen Vorzeichen geben müssen, sobald eine ungerade Anzahl von Wurzeln zwischen denselben belegen ist. Hieraus folgt nun:

Wenn f(a) und f(b) dasselbe Vorzeichen haben, so liegt eine gerade Anzahl von Wurzeln zwischen a und b; haben f(a) und f(b) verschiedene Vorzeichen, so liegt eine ungerade Anzahl von Wurzeln zwischen a und b.

Setzt man z. B. in eine Gleichung, deren letztes Glied $\pm a_n$ ist, für x nach und nach $-\infty$, 0 und $+\infty$ ein, erhält man für f(x)

$$\pm \quad \pm a_n \quad +,$$

indem man + für $x = -\infty$ erhält, wenn die Gleichung von geradem, —, wenn sie von ungeradem Grade ist; hieraus folgt, dass *eine Gleichung von ungeradem Grade wenigstens eine reelle Wurzel hat, deren Vorzeichen das entgegengesetzte des letzten Gliedes ist, während eine Gleichung von geradem Grade wenigstens eine positive und eine negative Wurzel hat, sobald das letzte Glied negativ ist.*

Satz von Descartes.

104. Wenn zwei auf einander folgende Glieder einer Gleichung dasselbe Vorzeichen haben, sagt man, dass sie eine Zeichenfolge (Permanenz) bilden; haben sie verschiedene Vorzeichen, bilden sie einen Zeichenwechsel (Variation). Descartes hat folgenden Satz aufgestellt:

Eine Gleichung hat nicht mehr positive Wurzeln als Zeichenwechsel, und nicht mehr negative Wurzeln als Zeichenfolgen.

Um diesen Satz zu beweisen werde eine beliebige auf gewöhnliche Weise geordnete Gleichung betrachtet und durch Multiplication mit $x - a$ die positive Wurzel a eingeführt; man kann dann zeigen, dass, wie die Vorzeichen auch sein mögen, nach ausgeführter Multiplication wenigstens ein Zeichenwechsel hinzugekommen ist.

Das erste Glied der Gleichung, x^n, ist positiv; den ersten Zeichenwechsel trifft man also, sobald man dem ersten negativen Gliede begegnet, da diesem ein positives Glied vorangehen muss; diese beiden Glieder seien

$$a_{n-p}\, x^p - a_{n-p+1}\, x^{p-1}.$$

Eines der Glieder der neuen Gleichung wird dann sein

$$-(a\, a_{n-p} + a_{n-p+1})\, x^p.$$

Ob das vorhergehende Glied positiv ist, weiss man nicht, aber man weiss, dass jedenfalls ein vorhergehendes positives Glied existirt, und dass man also, wenn man in der neuen Gleichung auf das Glied x^p trifft, wenigstens einen Zeichenwechsel hat, ebenso wie in der gegebenen Gleichung bei x^{p-1}. Sind es mehr, so müssen sie in ungerader Anzahl vorhanden sein, da eine Aenderung eines Vorzeichens die Anzahl derselben niemals um eine ungerade Zahl vermehren oder vermindern kann.

Der nächste Zeichenwechsel, welchem man in der gegebenen Gleichung begegnet, findet statt, wenn man nach

x^{p-1} auf einen positiven Coefficienten trifft; geschieht dies bei dem Gliede x^q, so sieht man auf dieselbe Weise wie oben, dass der Coefficient von x^{q+1} in der neuen Gleichung positiv ist, so dass man, welche Vorzeichen die zwischenliegenden Glieder auch haben mögen, wenigstens einen Zeichenwechsel in der neuen Gleichung hinzubekommen hat. Bei Fortsetzung dieses Verfahrens ist ersichtlich, dass man ebenso viele Zeichenwechsel, wie man angetroffen hat, als man in der gegebenen Gleichung das Glied x^r erreichte, wenigstens auch angetroffen haben muss, sobald man in der neuen Gleichung auf das Glied x^{r+1} trifft. Nun nehme man an, dass bei x^r der letzte Zeichenwechsel in $f(x) = 0$ stattfinde, und dass $+k$ der Coefficient von x^r sei; die folgenden Coefficienten haben dann alle dasselbe Vorzeichen wie k, und in der neuen Gleichung hat der Coefficient von x^{r+1} dasselbe Vorzeichen wie k, während das letzte Glied derselben, $-aa_n$, das entgegengesetzte Vorzeichen von k hat; geht man also von x^{r+1} weiter, so muss man wenigstens noch einen Zeichenwechsel antreffen, und da vorher wenigstens eben so viele Zeichenwechsel wie in der gegebenen Gleichung constatirt waren, ist also hiermit bewiesen, dass die Multiplication mit $x - a$ die Anzahl der Zeichenwechsel wenigstens um 1 vermehrt hat.

Man kann sich nun aus $f(x) = 0$ alle positiven Wurzeln durch Division mit den entsprechenden Factoren entfernt denken; die dadurch enstehende Gleichung hat alle negativen und complexen Wurzeln der ursprünglichen Gleichung, aber man weiss nichts über die Anzahl ihrer Zeichenwechsel; man führe nun wieder die positiven Wurzeln einzeln durch Multiplication mit den entsprechenden Factoren ein, und es ist bewiesen, dass, wie auch die ursprünglichen Vorzeichen sein mögen, für jede eingeführte positive Wurzel die Anzahl der Zeichenwechsel um wenigstens 1 vermehrt ist.

Wenn alle positiven Wurzeln eingeführt sind, hat man wieder die gegebene Gleichung, welche also wenigstens ebenso viele Zeichenwechsel wie positive Wurzeln haben muss.

Durch Vertauschung von x mit —x folgt der zweite Theil des Satzes.

Eine Gleichung n^{ten} Grades hat im Ganzen n Zeichenwechsel und Zeichenfolgen; *falls eine solche Gleichung lauter reelle Wurzeln hat, muss deshalb die Anzahl der Zeichenwechsel genau gleich der Anzahl der positiven, die Anzahl der Zeichenfolgen gleich der der negativen Wurzeln sein.* Wenn einer oder mehrere Coefficienten Null sind, kann man diese nach Belieben als positiv oder negativ rechnen, da eine unendlich kleine Aenderung eines Coefficienten keine Wurzel dazu bringen kann, das Vorzeichen zu wechseln. (Von dem Falle, wo eine Wurzel Null ist, kann abgesehen werden.) In diesem Falle kann man die Vorzeichen für die Coefficienten Null theils so wählen, dass man möglichst wenig Zeichenfolgen, theils so, dass man möglichst wenig Zeichenwechsel erhält. Steht ein Coefficient Null zwischen einem positiven und einem negativen Coefficienten, ist es gleichgültig, ob man denselben als + oder — liest, da

$$+ \ 0 \ -$$

einen Zeichenwechsel und eine Zeichenfolge giebt, welches Vorzeichen man auch Null geben möge. Steht 0 dagegen zwischen zwei Coefficienten mit gleichen Vorzeichen, so zeigt das immer das Vorhandensein von wenigstens zwei complexen Wurzeln an; hat man z. B.

$$+ \ 0 \ +,$$

kann man, wenn man die Zeichenwechsel zählt,

$$+ \ + \ +,$$

und wenn man die Zeichenfolgen zählt,

$$+ \ - \ +$$

lesen. Die Summe der erhaltenen Anzahlen der beiden wird dann um zwei geringer als die Anzahl der Wurzeln und zeigt also, dass die Gleichung wenigstens zwei complexe Wurzeln hat.

Wenn die gefundenen Zahlen nicht genau die Anzahl der positiven oder negativen Wurzeln geben, muss der Unterschied zwischen beiden eine gerade Anzahl sein; das folgt aus dem, was eben bei Einführung einer positiven Wurzel gezeigt wurde, indem man leicht sieht, dass eine Gleichung mit lauter complexen Wurzeln immer eine gerade Anzahl von Zeichenwechseln hat. (Das letzte Glied ist positiv.)

Beisp.

$$x^7 + x^6 - x^4 - 2x^3 - x + 1 = 0.$$

Man kann

$$+ + + - - - - +$$

oder

$$+ - + - - + - +$$

lesen, so dass die Gleichung höchstens zwei positive und eine negative Wurzel hat; sie muss deshalb wenigstens vier complexe Wurzeln haben.

Satz von Budan.

105. Die Sätze von Descartes und Newton sind mit einbegriffen in einen Satz von Budan; dieser Satz wird auch Fourier zugeschrieben, der denselben in seinen Vorlesungen mitgetheilt haben soll, bevor Budan denselben veröffentlichte. Man bilde die Reihe

$$f(x),\ f'(x),\ f''(x) \ldots f^{(n)}(x),$$

und setze $x = a$ und $x = b$ ein, wo $a < b$.

Die Gleichung hat dann nicht mehr Wurzeln zwischen a und b als die Reihe Zeichenwechsel verliert, wenn man von a zu b übergeht.

Man sieht leicht, dass, wenn eine der Functionen für ein wachsendes x durch Null hindurchgeht, für diese und die folgende ein Zeichenwechsel in eine Zeichenfolge übergehen muss; betrachtet man z. B. $f^{(p)}(x)$, so hat man

$$f^{(p)}(x-h) = f^{(p)}(x) - f^{(p+1)}(x)\,h + \ldots$$

$$f^{(p)}(x+h) = f^{(p)}(x) + f^{(p+1)}(x)\,h + \ldots;$$

für $f^{(p)}(x) = 0$ und ein hinreichend kleines h haben also

$$f^{(p)}(x-h) \text{ und } f^{(p+1)}(x)$$

verschiedene Vorzeichen; $f^{(p+1)}(x)$ hat indessen dasselbe Vorzeichen wie $f^{(p+1)}(x-h)$, wenn nur nicht $f^{(p+1)}(x)$ und $f^{(p)}(x)$ gleichzeitig Null sind; wenn also zwei auf einander folgende abgeleitete Functionen nicht gleichzeitig Null sind, muss, wenn die erste verschwindet, ein Zeichenwechsel zwischen dieser und der folgenden verloren werden. Betrachtet man nun die drei Functionen

$$f^{(p-1)}(x),\ f^{(p)}(x),\ f^{(p+1)}(x),$$

sieht man, dass, wenn $f^{(p)}(x)$ durch Null hindurchgeht, ein Zeichenwechsel durch die beiden letzten verloren wird, während durch die beiden ersten ein Zeichenwechsel verloren oder gewonnen werden kann; indem also $f^{(p)}(x)$ durch Null hindurchgeht, müssen zwei oder keine Zeichenwechsel verloren werden; doch wird, wenn f(x) durch Null hindurchgeht immer ein Zeichenwechsel verloren werden, da hier keine vorhergehende Function existirt. Das Resultat ist folglich, *dass man wenigstens einen Zeichenwechsel verliert für jede Wurzel der Gleichung, welche man passirt, dass man mehr verlieren kann, und dass diese dann immer paarweise verloren werden.*

106. Der Fall, wo zwei oder mehrere auf einander folgende Functionen gleichzeitig Null werden, muss besonders

betrachtet werden; $f^{p-1}(x)$ sei die letzte dieser Functionen; dann hat man

$$f^{(p-1)}(x-h) = -f^{(p)}(x)h + \ldots, \quad f^{(p-1)}(x+h) = f^{(p)}(x)h + \ldots,$$

$$f^{(p-2)}(x-h) = +f^{(p)}(x)\frac{h^2}{1.2} + \ldots, \quad f^{(p-2)}(x+h) = f^{(p)}(x)\frac{h^2}{1.2} + \ldots,$$

$$f^{(p-3)}(x-h) = -f^{(p)}(x)\frac{h^3}{1.2.3} + \ldots, \quad f^{(p-3)}(x+h) = f^{(p)}(x)\frac{h^3}{1.2.3} + \ldots,$$

....

....

während also die Functionen, welche gleichzeitig Null werden, und die erste, welche nicht Null wird, früher lauter Zeichenwechsel gaben, geben sie jetzt lauter Zeichenfolgen, so dass auch in diesem Falle ein Verlust von Zeichenwechseln stattfindet. Besondere Bedeutung hat der Fall, wo die p ersten Glieder der Reihe gleichzeitig Null werden; in diesem Falle hat die Gleichung p gleiche Wurzeln, welche alle auf einmal passirt werden, und wie gezeigt worden, gehen dabei p Zeichenwechsel verloren. Der Satz gilt also für alle Fälle, und namentlich auch für mehrfache Wurzeln.

Setzt man $-\infty$ für x ein, so hat die Reihe lauter Zeichenwechsel, setz man 0 ein, so erhält man dieselbe Reihe von Vorzeichen, welche die Coefficienten der Gleichung haben, setzt man $+\infty$ ein, so giebt die Reihe lauter Zeichenfolgen. Hierdurch wird, ebenso wie durch den Satz von Descartes, die grösstmögliche Anzahl von negativen oder positiven Wurzeln bestimmt.

Setzt man einen Werth k ein, welcher lauter Zeichenfolgen giebt, so kann zwischen k und $+\infty$ keine Wurzel liegen; k ist also eine obere Grenze der Wurzeln, so dass auch Newton's Satz in den von Budan mit einbegriffen ist.

Wenn f(a) und f(b) verschiedene Vorzeichen haben, während alle übrigen Functionen dasselbe Vorzeichen für $x = a$ und $x = b$ bekommen, *liegt eine und nur eine Wurzel zwischen a nnd b,* denn es ist gezeigt worden, dass zwischen a und b eine ungerade Anzahl von Wurzeln liegen muss, und es ist nur ein Zeichenwechsel verloren. Die Wurzel ist also in diesem Falle zwischen a und b abgesondert. Man muss

indessen beachten, dass man auf diese Weise eine Wurzel nicht sicher absondern kann, da zwischen a und b Werthe liegen können, welche einige der abgeleiteten Functionen zu Null machen und dadurch verursachen, dass beim Uebergange von a zu b mehr als ein Zeichenwechsel verloren wird.

Durch die benutzte Reihe ist man im Stande die grösstmögliche Anzahl reeller Wurzeln innerhalb eines gewissen Intervalles zu bestimmen; begreiflicher Weise ist es nicht möglich, allein aus den Vorzeichen dieser Reihe die Anzahl der complexen Wurzeln zu bestimmen, denn beim Uebergange von $x = -\infty$ zu $x = +\infty$ erhält man dieselben Veränderungen der Vorzeichen, einerlei ob die Gleichung complexe Wurzeln hat oder nicht.

Satz von Rolle.

107. *Wenn a und b zwei Wurzeln der Gleichung $f(x) = 0$ sind und zwischen a und b keine Wurzel existirt, muss die Gleichung $f'(x) = 0$ eine ungerade Anzahl Wurzeln (also wenigstens eine Wurzel) zwischen a und b haben.*

Da nämlich $f(x)$ eine continuirliche Function ist, kann dieselbe, da sie für $x = a$ und $x = b$ Null wird, nicht beständig wachsen oder beständig abnehmen, wenn x von a zu b übergeht; sie muss also ein Maximum oder Minimum für einen Werth von x haben, welcher zwischen a und b liegt, und dieser Werth muss dann eine Wurzel von $f'(x) = 0$ sein.

Die Function kann mehrere Maxima und Minima zwischen a und b haben, aber, da sie nicht das Vorzeichen wechselt, muss sie nothwendig, wenn sie anfangs wächst, schliesslich abnehmen, und umgekehrt; man sieht leicht, dass dieses das Vorhandensein einer ungeraden Anzahl Maxima oder Minima mit sich bringt. Eine Betrachtung der Curve $y = f(x)$ wird das hier entwickelte leicht anschaulich machen.

Hieraus folgt, *dass zwischen zwei auf einander folgenden Wurzeln von $f'(x) = 0$ höchstens eine Wurzel von $f(x) = 0$ liegen kann,* denn wenn dort zwei lägen, müsste zwischen diesen eine Wurzel von $f'(x) = 0$ liegen; ferner folgt, dass *wenn $f(x) = 0$ lauter reelle Wurzeln hat, auch $f'(x) = 0$ lauter reelle Wurzeln hat,* und dass, *wenn $f(x) = 0$ für $x = a$ p gleiche Wurzeln hat, $f'(x)$ für denselben Werth von x $p-1$ gleiche Wurzeln haben muss.*

Beisp.

$$f(x) = x^m + p x^n + q = 0. \quad \text{(m und n ungerade Zahlen.)}$$

Die Regel von Descartes zeigt, dass die Gleichung 1 oder 2 reelle Wurzeln haben muss. Nun ist

$$f'(x) = m x^{n-1}\left(x^{m-n} + \frac{np}{m}\right).$$

1. *p ist positiv.* $f'(x) = 0$ hat keine reelle Wurzel ausser $x = 0$. $f(x) = 0$ hat deshalb nur eine reelle Wurzel.

2. *p ist negativ.* $f'(x) = 0$ hat ausser $x = 0$ zwei reelle Wurzeln; bezeichnet man diese mit $-b$ und $+b$, kann $f(x) = 0$ drei reelle Wurzeln haben, die in den Intervallen ($n-1$ ist gerade)

$$-\infty, \; -b, \; +b, \; -\infty$$

belegen sind; ist dies der Fall, so müssen diese Werthe, in $f(x)$ eingesetzt, die Vorzeichen $- + - +$ geben. Die Bedingung hierfür ist

$$-p b^n - b^m > \pm q,$$

oder, nach Einsetzung des Werthes von b und einer kleinen Umformung

$$\left(\frac{nq}{m-n}\right)^{m-n} + \left(\frac{np}{m}\right)^m < 0.$$

Für die Gleichung

$$x^3 + px + q = 0$$

wird dadurch die Bedingung für drei reelle Wurzeln

$$4p^3 + 27q^2 < 0.$$

Satz von Sturm.

108. Bei Budan's Satz wurde bemerkt, dass die Ursache, welche es verhindert die genaue Anzahl von reellen Wurzeln innerhalb eines gegebenen Intervalls zu bestimmen, darin liegt, dass ein Glied der Reihe, indem es durch Null hindurchgeht, zwischen zwei Gliedern mit demselben Vorzeichen liegt und dadurch einen Verlust an Zeichenwechseln verursachen kann, welcher die Wurzeln der Gleichung nicht berührte. Diese Schwierigkeit hat Sturm überwunden, indem er eine andere Reihe benutzte, die eben die Eigenschaft hat, dass ein Glied derselben, indem es durch Null hindurch geht, immer zwischen zwei Gliedern mit entgegengesetztem Vorzeichen liegt und also nicht durch sein Verschwinden die Anzahl der Zeichenwechsel verändern kann. Die Sturmsche Reihe beginnt wie die von Budan mit $f(x)$ und $f'(x)$, aber die folgenden Glieder der Reihe werden aus diesen durch das Verfahren gebildet, welches man einschlägt, um den grössten gemeinschaftlichen Factor für $f(x)$ und $f'(x)$ zu suchen; hierbei ist indessen zu beachten, dass man bei den Divisionen *jedesmal das Vorzeichen des Restes ändert,* und *dass man nur positive Factoren einführen darf* um Brüche zu vermeiden. Die Gleichung wird als von mehrfachen Wurzeln befreit angenommen, so dass $f(x)$ und $f'(x)$ keinen gemeinschaftlichen Factor haben, und der letzte Rest unabhängig von x wird. Die Glieder der Reihe sind dann also

$f(x)$, $f'(x)$ und die Divisionsreste mit umgekehrten Vorzeichen; sie mögen mit

$$f(x),\ f'(x),\ f_2(x),\ f_3(x) \ldots f_n(x)$$

bezeichnet werden; dann hat man, wenn man die Quotienten mit q und die eingeführten positiven Factoren mit c bezeichnet,

$$\begin{aligned} c\, f(x) &= q\, f'(x) - f_2(x), \\ c_1\, f'(x) &= q_1\, f_2(x) - f_3(x), \\ c_2\, f_2(x) &= q_2\, f_3(x) - f_4(x), \\ &\ldots\ldots\ldots\ldots \\ &\ldots\ldots\ldots\ldots \\ c_{n-2}\, f_{n-2}(x) &= q_{n-2}\, f_{n-1}(x) - f_n(x). \end{aligned}$$

Ueber diese Reihe gelten nun folgende Sätze:

Zwei auf einander folgende Glieder können nicht für denselben Werth von x verschwinden. Das würde nämlich mit sich führen, dass alle für diesen Werth gleich Null würden, und die Gleichung müsste dann gleiche Wurzeln haben.

Wenn ein Glied der Reihe [ausgenommen $f(x)$] gleich Null wird, liegt es zwischen zwei Gliedern, welche verschiedene Vorzeichen haben; z. B. für $f_3(x) = 0$ hat man $c_2\, f_2(x) = - f_4(x)$ u. s. w.

Denkt man sich nun x von $-\infty$ bis $+\infty$ wachsend, können die Vorzeichen der Reihe nur verändert werden, sobald eines der Glieder gleich Null wird. Dadurch wird indessen kein Zeichenwechsel verloren, da das Glied, indem es gleich Null wird, zwischen zwei Gliedern mit verschiedenen Vorzeichen liegt, so dass diese drei Glieder, sowohl bevor als auch nachdem das mittlere sein Vorzeichen verändert hat, einen Zeichenwechsel und eine Zeichenfolge geben. Dieses gilt nicht für das letzte und erste Glied der Reihe, da diese nicht zwischen zwei anderen liegen; aber das letzte Glied ist unabhängig von x und kann deshalb sein Vorzeichen nicht wechseln, und mit Rücksicht auf das erste Glied $f(x)$ folgt aus 105, dass ein Zeichenwechsel verloren wird, sobald es sein Vorzeichen wechselt. Die Reihe verliert also genau einen Zeichenwechsel für jede Wurzel, durch welche man hindurch geht; also

Setzt man in die Sturmsche Reihe $x = a$ und $x = b$ ein, so wird die Anzahl der verlorenen Zeichenwechsel genau gleich der Anzahl der Wurzeln sein, welche zwischen a und b liegen.

Wenn der eingesetzte Werth zufälligerweise eines der Glieder der Reihe, welche auf das erste folgen, gleich Null macht, kann man hier nach Belieben + oder — lesen. Wird das erste Glied Null, so hat man eine Wurzel der Gleichung; ist der eingesetzte Werth die untere Grenze, beginnt man also die Reihe mit einem Zeichenwechsel, ist er die obere Grenze, mit einer Zeichenfolge, wenn man diese Wurzel mitzählen will. Falls ein Glied der Reihe keinen Zeichenwechsel innerhalb des betrachteten Intervalls erleidet, kann man bei diesem stehen bleiben; der Beweis fordert nämlich nur, dass das letzte Glied der Reihe das Vorzeichen nicht ändert; wird diese Bedingung erfüllt, so ist es gleichgültig, ob das Glied x enthält oder nicht.

109. Da man bei Bildung der Sturmschen Reihe den grössten gemeinschaftlichen Factor für $f(x)$ und $f'(x)$ findet, wird es sich bei der Rechnung herausstellen, ob gleiche Wurzeln vorhanden sind oder nicht; durch etwa vorhandene gleiche Wurzeln würden alle Glieder der Reihe einen gemeinschaftlichen Factor φ bekommen, und dieser kann durch Division entfernt werden, ohne dass die Eigenschaften der Reihe, auf welche der geführte Beweis sich stützt, verändert würden; das letzte Glied ist jetzt ebenso wie vorher constant, die beiden ersten $\frac{f(x)}{\varphi}$ und $\frac{f'(x)}{\varphi}$, verlieren einen Zeichenwechsel, wenn $f(x)$ und $f'(x)$ durch Null hindurchgehen, und im Uebrigen liegt jedes Glied der Reihe, indem es durch Null hindurchgeht, zwischen zwei Gliedern mit entgegengesetzten Vorzeichen. Nach ausgeführter Division kann dann der Satz von Sturm benutzt werden, *aber alle gleichen Wurzeln von gleicher Grösse zählen dann nur jedesmal wie eine Wuvzel.* Man braucht nicht einmal durch den Factor zu dividiren, denn wenn derselbe für den eingesetzten Werth positiv ist, kann er die Vorzeichen der Glieder nicht verändern, während

er, wenn er negativ ist, alle Vorzeichen der Reihe umkehrt, eine Veränderung, welche auf die Anzahl der Zeichenwechsel keinen Einfluss haben kann.

Hat die gegebene Gleichung n^{ten} Grades lauter reelle und ungleich grosse Wurzeln, so muss die Reihe $n+1$ Glieder erhalten, welche für $x = -\infty$ lauter Zeichenwechsel, für $x = +\infty$ lauter Zeichenfolgen geben. Die Bedingung hierfür ist, dass jede der Functionen mit einem Gliede mit positivem Coefficienten anfängt.

Setzt man $x = -\infty$ und $x = 0$ in die Sturmsche Reihe ein, so findet man die Anzahl der negativen Wurzeln einer Gleichung; durch Einsetzen von $x = 0$ und $x = +\infty$ findet man die Anzahl der positiven Wurzeln; die fehlenden Wurzeln sind dann complex.

Beisp. 1.

$$x^6 + 3x^4 - 4x^3 + 6x^2 + 12x - 18 = 0.$$

Man erhält, wenn man positive Factoren fortlässt:

	$-\infty$	$+\infty$	0
$f(x) = x^6 + 3x^4 - 4x^3 + 6x^2 + 12x - 18$	+	+	—
$\frac{1}{6} f'(x) = x^5 + 2x^3 - 2x^2 + 2x + 2$	—	+	+
$f_2(x) = -x^4 + 2x^3 - 4x^2 - 10x + 18$	—	—	+
$f_3(x) = -x^3 + 10x^2 - 119$	+	—	—
$f_4(x) = 84x^2 - 9x - 170$	+	+	—
$f_5(x) = 2267x - 2402$	—	+	—
$f_6(x) = \quad +$	+	+	+

Für $x = -\infty$ hat man vier, für $x = 0$ drei, und für $x = +\infty$ zwei Zeichenwechsel. Die Gleichung hat also eine negative, eine positive und vier complexe Wurzeln.

Beisp. 2.

$$x^3 + ax + b = 0.$$

$$f(x) = x^3 + ax + b$$
$$f'(x) = 3x^2 + a$$
$$f_2(x) = -2ax - 3b$$
$$f_3(x) = -4a^3 - 27b^2.$$

Die Bedingungen für drei reelle Wurzeln sind ein negatives a und

$$4a^3 + 27b^2 < 0,$$

von denen die erste in der letzten mit einbegriffen ist; ist diese erfüllt, erhält man für $x = 0$

$$b, \; a, \; -3b, \; +,$$

wo die drei ersten immer einen Zeichenwechsel und eine Zeichenfolge geben; man hat also zwei positive und eine negative Wurzel, wenn b positiv ist, zwei negative und eine positive, wenn b negativ ist.

Anwendung des Sturmschen Satzes auf complexe Wurzeln.

110. Es ist früher gezeigt worden, dass eine Gleichung

$$f(z) = 0$$

mit reellen oder imaginären Coefficienten, wenn man

$$z = x + yi$$

setzt, sich in zwei andere

$$A = 0 \text{ und } B = 0$$

theilt, welche als die Gleichungen zweier Curven aufgefasst werden können, deren Durchschnittspunkte, die Wurzelpunkte, die Wurzeln der Gleichung darstellen. Es soll versucht werden, die Anzahl solcher Wurzelpunkte zu bestimmen, welche innerhalb einer gegebenen geschlossenen Curve belegen sind; der Einfachheit wegen mag es genügen, die Anzahl der Wurzeln in einem Kreise zu suchen, dessen Radius r und dessen Mittelpunkt durch die Coordinaten a, b gegeben ist. Die Gleichung dieses Kreises kann ersetzt werden durch die beiden Gleichungen

$$x = a + r\frac{1 - t^2}{1 + t^2}; \; y = b + r\frac{2t}{1 + t^2},$$

welche durch Elimination von t eben die Gleichung des Kreises geben.

Die Kreisperipherie wird dann in einer bestimmten Umlaufsrichtung durchlaufen, wenn man t von $-\infty$ bis $+\infty$ wachsen lässt. Zufolge des Satzes von Cauchy wird die Anzahl der Wurzelpunkte innerhalb des Kreises halb so gross sein wie der Unterschied zwischen den beiden Zahlen, welche angeben, wie oft AB vom Positiven zum Negativen übergeht und umgekehrt, wenn man die Curve A passirt. Diese Zahlen sind dieselben wie die, welche, wenn A und B hinter einander mit ihren Vorzeichen geschrieben werden, angeben, wie oft beim Passiren von A eine Zeichenfolge in einen Zeichenwechsel und wie oft ein Zeichenwechsel in eine Zeichenfolge übergeht.

Nun führe man in A und B für x und y t ein und multiplicire beide mit derselben Grösse, so dass man zwei relativ prime ganze Polynome in t bekommt; aus diesen bilde man eine Reihe wie früher aus f(x) und f′(x), und untersuche darauf, wie viele Zeichenwechsel diese Reihe verliert, wenn t von $-\infty$ zu $+\infty$ übergeht. Weil die Reihe so gebildet ist, dass ein Glied, wenn es gleich Null wird, zwischen zwei Gliedern mit verschiedenen Vorzeichen liegt, während das letzte Glied der Reihe sein Vorzeichen nicht verändern kann, müssen die verlorenen (oder gewonnenen) Zeichenwechsel allein von den Stellen herrühren, wo das erste Glied der Reihe durch Null hindurchgeht. Die Anzahl der verlorenen Zeichenwechsel giebt also den Unterschied zwischen der Anzahl Male an, wo das Product der beiden ersten Glieder der Reihe vom Negativen zum Positiven, und der Anzahl Male, wo es vom Positiven zum Negativen übergeht, während das erste Glied durch Null hindurch geht. Da nun der Umstand, dass A und B mit derselben Grösse multiplicirt worden sind, nicht das Vorzeichen ihres Productes verändern kann, so sieht man, *dass für jeden Wurzelpunkt innerhalb des Kreises zwei Zeichenwechsel verloren (oder gewonnen) werden.*

Absonderung der reellen Wurzeln.

111. Nach dem Vorhergehenden lässt sich leicht entscheiden, ob zwischen zwei gegebenen Zahlen eine gerade oder ungerade Anzahl Wurzeln liegt. Bevor man aber zur numerischen Berechnung der Wurzeln schreiten kann, muss man solche Intervalle bestimmen, innerhalb welcher die Wurzeln einzeln belegen sind. In besonderen Fällen kann eine Wurzel ohne Schwierigkeit abgesondert werden; wenn z. B. alle Glieder von f(x) mit Ausnahme des letzten positiv sind, hat die Gleichung nur eine positive Wurzel, und diese ist also vollständig abgesondert; setzt man für x

$$1, 10, 100 \ldots$$

ein, so kann man zwei von diesen Zahlen bestimmen, zwischen welchen die Wurzel liegt, und man kann dann ferner durch Probiren die Grenzen einschränken bis man die beiden auf einander folgenden ganzen Zahlen gefunden hat, zwischen denen die Wurzel liegt. Die Anzahl der Versuche lässt sich vermindern, indem man durch eine der früher angegebenen Methoden zuerst die obere und untere Grenze der Wurzel bestimmt.

Eine sichere aber sehr mühsame Methode für die Absonderung der Wurzeln ist von Waring und später von Lagrange angegeben worden. Man bildet die der Gleichung entsprechende Gleichung der quadrirten Wurzeldifferenzen. Für diese Gleichung bestimmt man die untere Grenze der positiven Wurzeln; diese sei α ; dann hat man für zwei beliebige reelle Wurzeln der gegebenen Gleichuug

$$x_p - x_q > \sqrt{\alpha}.$$

Bildet man nun eine beliebige Differenzenreihe mit der Differenz $\sqrt{\alpha}$, z. B.

$$\sqrt{\alpha}, 2\sqrt{\alpha}, 3\sqrt{\alpha} \ldots,$$

so kann zwischen zwei Gliedern dieser Reihe nicht mehr

als eine Wurzel der gegebene Gleichung liegen, denn, wenn es zwei wären, müsste ihre Differenz kleiner als $\sqrt{\alpha}$ sein.

Die Methode setzt natürlich voraus, dass man zuerst die Gleichung von gleichen Wurzeln befreit, da man im entgegengesetzten Falle $\alpha = 0$ erhalten würde.

Diese Methode kann allerdings so verändert werden, dass man nur nöthig hat das letzte Glied der Gleichung der quadrirten Wurzeldifferenzen zu bilden; von einer genaueren Ausführung kann hier aber abgesehen werden, da der Satz von Sturm die Möglichkeit bietet, die Wurzeln auf leichtere Weise abzusondern.

Um die Wurzeln abzusondern bilde man die Sturmsche Reihe und setze für x eine Reihe Werthe ein, zwischen welchen man neue einschaltet, bis man beim Uebergange von einem Werthe zu dem nächst höheren nur einen Zeichenwechsel verliert; die Wurzeln sind dann vollständig abgesondert, und die Grenzen können dann durch blosses Probiren an der gegebenen Gleichung enger gemacht werden.

Beisp.

$$x^4 + x^3 - 4x^2 - 4x + 1 = 0.$$

Die Reihe wird

	$-\infty$	-2	-1	0	$+1$	$+2$
$x^4 + x^3 - 4x^2 - 4x + 1$	+	+	+	+	—	+
$4x^3 + 3x^2 - 8x - 4$	—	—	+	—	—	+
$7x^2 + 8x - 4$	+	+	—	—	+	+
$4x + 5$	—	—	+	+	+	+
+	+	+	+	+	+	+

Die Tabelle zeigt, dass beim Uebergange von -2 zu -1, von 0 zu 1 und von 1 zu 2 beziehungsweise 2, 1 und 1 Zeichenwechsel verloren werden. Die Gleichung hat also vier reelle Wurzeln, von denen die beiden positiven vollständig abgesondert sind; um die beiden Wurzeln zwischen -2 und -1 abzusondern, setze man $x = -\frac{3}{2}$ in die ge-

gebene Gleichung ein, wodurch man ein negatives Resultat erhält; die eine negative Wurzel liegt also zwischen -1 und $-1,5$, die andere zwischen $-1,5$ und -2.

Methode von Fourier.

112. Mit Hülfe des Sturmschen Satzes kann man allerdings mit vollkommener Sicherheit die Wurzeln absondern, aber die Rechnungen werden bei dieser Methode auch leicht sehr beschwerlich; es kann z. B. sehr leicht eintreffen, dass man bei einer Gleichung 6ten oder 7ten Grades mit sehr einfachen Coefficienten zu Zahlen von 50 und mehr Ziffern gelangt; in der Praxis sucht man sich deshalb oft dadurch zu helfen, dass man den Satz von Budan auf eine von Fourier angegebene Weise benutzt.

Man wird sich erinnern, dass die von Budan benutzte Reihe

$$f(x), f'(x), f''(x) \ldots$$

war, dass diese Reihe ebenso wie die von Sturm benutzt wird, aber dass sie durch den Verlust von Zeichenwechseln nur eine obere Grenze für die Anzahl der reellen Wurzeln, welche man passirt hat, angiebt. Man verliert nämlich nicht nur jedesmal einen Zeichenwechsel, wenn $f(x)$ durch Null hindurchgeht, sondern man verliert jedesmal zwei Zeichenwechsel, wenn ein anderes Glied der Reihe durch Null hindurchgeht und gleichzeitig zwischen zwei Gliedern mit gleichen Vorzeichen liegt. Da man nun beim Uebergange von $-\infty$ zu $+\infty$ n Zeichenwechsel verliert, wenn die Gleichung vom n^{ten} Grade ist, muss die Gleichung zwei complexe Wurzeln für jede zwei Zeichenwechsel haben, welche verloren werden, wenn $f'(x)$ und $f''(x)$ und die folgenden durch Null hindurchgehen. Man kann deshalb mit Sicherheit schliessen, dass, wenn man beim Uebergange von $x = a$ zu $x = b$ keinen Zeichenwechsel verliert, die Gleichung keine

Wurzeln zwischen a und b hat, und dass die Gleichung eine Wurzel zwischen a und b hat, wenn man einen Zeichenwechsel verliert; verliert man dagegen zwei Zeichenwechsel, so kann das entweder bedeuten, dass die Gleichung zwei complexe, oder dass sie zwei reelle Wurzeln zwischen a und b hat.

113. Nun nehme man an, dass man ein Intervall gefunden habe, innerhalb dessen nur zwei Zeichenwechsel verloren würden, und dass dieses bei den drei ersten Gliedern der Reihe geschehe; dann hat man, wenn f(x) für die beiden Grenzen α und β ($\beta > \alpha$) des Intervalls positiv ist,

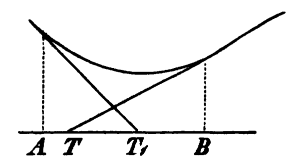
$$\begin{array}{ccc} f(\alpha) & f'(\alpha) & f''(\alpha) \\ + & - & + \end{array} \qquad \begin{array}{ccc} f(\beta) & f'(\beta) & f''(\beta). \\ + & + & + \end{array}$$

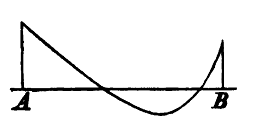
Da in dem übrigen Theil der Reihe keine Zeichenwechsel verloren werden, kann $f''(x) = 0$ keine Wurzeln zwischen α und β haben. $f''(x)$ ist also innerhalb des ganzen Intervalles positiv; wenn nun auch $f(x)$ innerhalb des ganzen Intervalles positiv ist, muss der Verlust von Zeichenwechseln angeben, dass zwei complexe Wurzeln vorhanden sind. Wie das allgemein entschieden werden kann, wird anschaulicher durch eine geometrische Betrachtung.

Da die Durchschnittspunkte der Curve

$$y = f(x)$$

mit der x-Axe eben durch die gegebene Gleichung bestimmt werden, gilt es zu entscheiden, ob zwischen $x = \alpha$ und $x = \beta$ zwei oder keine Durchschnittspunkte vorhanden sind. Da $f'(x)$ das Vorzeichen wechselt, während $f''(x)$ innerhalb des Intervalles positiv ist, so existirt innerhalb desselben ein Minimum und die Concavität ist nach oben gewendet; die beiden Fälle werden also durch die nebenstehenden Figuren repräsentirt,





von denen die erste dem Falle entspricht, wo zwei complexe Wurzeln, die zweite dem, wo zwei reelle Wurzeln vorhanden sind. Schneiden sich nun die Tangenten an die beiden Grenzpunkte oberhalb der Axe, so muss man bestimmt complexe Wurzeln haben, während man den entgegesetzten Schluss nicht machen darf. Es müssen also complexe Wurzeln vorhanden sein, sobald $AT_1 + TB \geqq AB$, dass heisst, sobald

$$\frac{f(\beta)}{f'(\beta)} - \frac{f(\alpha)}{f'(\alpha)} \geqq \beta - \alpha \ldots\ldots\ldots\ldots \quad (1)$$

Man darf, wie gesagt, nicht schliessen, dass die Wurzeln reell sind, sobald der Durchschnittspunkt der Tangenten unterhalb der Axe fällt, aber man sieht, dass, wenn die Wurzeln complex sind, man immer α und β einander so weit wird nähern können, dass der Durchschnittspunkt oberhalb der Axe fällt. Man theilt deshalb das Intervall zwischen α und β so lange, bis man die Bedingung (1) erfüllt bekommt, oder bis statt des Verlustes von zwei Zeichenwechseln zweimal ein Verlust von einem Zeichenwechsel erfolgt; im ersten Falle hat man complexe, im zweiten reelle Wurzeln. Natürlich ist dabei vorausgesetzt, dass keine gleichen Wurzeln vorhanden sind.

114. Nun kann man den allgemeinen Fall betrachten und annehmen, dass die Reihe beim Uebergange von α zu β d Zeichenwechsel verliere; lässt man das erste Glied aus, das heisst, betrachtet man $f'(x) = 0$ als die gegebene Gleichung, so verliert man d_1 Zeichenwechsel, für $f''(x) = 0$ verliert man d_2 Zeichenwechsel u. s. w. Zwei auf einander folgende d müssen dann gleich gross sein, oder ihr Unterschied muss 1 betragen. Fourier nennt d_p den $f^{(p)}(x)$ entsprechenden Index.

Nun nehme man den ersten Index der Reihe, welcher 1 ist; derselbe sei d_p. $f^{(p)}(x) = 0$ hat dann eine reelle Wurzel zwischen α und β. Der vorhergehende Index muss 2 sein, denn wäre er 0, müsste schon ein Index 1 vorhergehen; der

nachfolgende Index kann 2, 1 oder 0 sein; ist er 2 oder 1, kann das Intervall immer in kleinere getheilt werden, so dass das Intervall, welches die Wurzel von $f^{(p)}(x) = 0$ enthält, keine Wurzel von $f^{(p+1)}(x) = 0$ enthält; für die übrigen Intervalle hat man dann

$$d_p = 0,$$

und der erste Index 1 ist dann weiter links in der Reihe zu suchen; man hat also nur nöthig den Fall zu betrachten, wo

$$d_{p-1} = 2,\ d_p = 1,\ d_{p+1} = 0.$$

Dieser Fall stimmt mit dem in 113 betrachteten überein, und man kann dann auf die dort angegebene Weise entscheiden, ob die beiden Wurzeln von

$$f^{(p-1)}(x) = 0$$

reell oder complex sind; sind sie reell, so kann man das Intervall in zwei theilen, von denen jedes eine Wurzel enthält, und da jedes von diesen den Index 1 erhält, kann man auf dieselbe Weise fortfahren; sind sie complex, so müssen die beiden Zeichenwechsel dadurch verloren sein, dass eine der folgenden Functionen, indem sie durch Null hindurchgeht, zwischen zwei anderen mit gleichen Vorzeichen liegt; die gegebene Gleichung muss dann auch zwei complexe Wurzeln haben, und lässt man diese von der Betrachtung aus, kann man 2 von jedem Index in dem Theil der Reihe, welcher noch zu untersuchen ist, abziehen. Verfährt man auf diese Weise, kann man also nach und nach den ersten Index 1 weiter nach einem früheren Gliede der Reihe zurückschieben; ist er bis an das erste Glied der Reihe geschoben, ist die Wurzel abgesondert.

Beisp.

$$x^5 - 5x^4 - 16x^3 + 12x^2 - 9x - 5 = 0.$$

Man hat

$$f(x) = x^5 - 5x^4 - 16x^3 + 12x^2 - 9x - 5$$
$$f'(x) = 5x^4 - 20x^3 - 48x^2 + 24x - 9$$
$$\frac{1}{4} f''(x) = 5x^3 - 15x^2 - 24x + 6$$
$$\frac{1}{12} f'''(x) = 5x^2 - 10x - 8$$
$$\frac{1}{120} f^{IV}(x) = x - 1$$
$$f^{V}(x) \qquad +$$

Die obere Grenze der Wurzeln ist 8. Für das Intervall von 0 bis 8 hat man einen Verlust von drei Zeichenwechseln, von denen zwei von 0 bis 1, der eine von 7 bis 8 verloren wird. Eine Wurzel ist also zwischen 7 und 8 abgesondert, während das Intervall von 0 bis 1 genauer untersucht werden muss. Die Vorzeichen der Reihe sind

$$x = 0; \; - - + - - +$$
$$x = 1; \; - - - - - +,$$

wenn man 0 als — liest; dann hat man

$$d_1 = 2, \; d_2 = 1, \; d_3 = 0$$

und

$$\frac{f'(1)}{f''(1)} - \frac{f'(0)}{f''(0)} = \frac{3}{7} + \frac{3}{8} < 1,$$

so dass man die Grenzen enger machen muss; man setze also $\beta = \frac{1}{2}$ und erhält

$$- - - - - +,$$

woraus man sieht, dass die Zeichenwechsel von 0 bis $\frac{1}{2}$ verloren werden; nun findet man

$$\frac{f'\left(\frac{1}{2}\right)}{f''\left(\frac{1}{2}\right)} - \frac{f'(0)}{f''(0)} > \frac{1}{2},$$

woraus hervorgeht, dass die beiden Wurzeln complex sind. Die Gleichung hat ausserdem zwei negative Wurzeln, von

denen die eine zwischen -3 und -2, die andere zwischen -1 und 0 abgesondert wird.

115. Die complexen Wurzeln können durch die in 110 angegebene Methode abgesondert werden, oder dadurch, dass man den dort angewendeten Kreis einmal durch zwei der y-Axe parallele Gerade ersetzt, wodurch der reelle Theil der Wurzeln abgesondert wird, dann durch zwei der x-Axe parallele Gerade, wodurch der imaginäre Theil abgesondert wird.

Satz von Newton.

116. Newton hat einen Satz ohne Beweis aufgestellt, welcher später von Sylvester bewiesen und erweitert worden ist, der eine Correction für die durch Budan's Satz bestimmte Anzahl Wurzeln innerhalb gegebener Grenzen abgiebt.

Mit Budan's Reihe wird eine andere Reihe verbunden, welche der ersteren Glied für Glied entspricht. Wenn man in der ersten Reihe einen Zeichenwechsel hat, während die entsprechenden Glieder der zweiten Reihe eine Zeichenfolge geben, so hat man eine sogenannte Variation-Permanenz, die für die Folge mit V-P*) bezeichnet werden soll.

Wenn $f(x) = 0$ vom n^{ten} Grade ist, sind die beiden Reihen

$$\left.\begin{array}{l} f(x),\ f^2(x) \\ f'(x),\ \left(f'(x)\right)^2 - k_1 f(x) f''(x) \\ f''(x),\ \left(f''(x)\right)^2 - k_2 f'(x) f'''(x) \\ \cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots \\ f^{(p)}(x),\ \left(f^{(p)}(x)\right)^2 - k_p f^{(p-1)}(x) f^{(p+1)}(x) \\ \cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots \end{array}\right\}, \ldots\ldots (1)$$

---

*) Es hätte sich leicht ein entsprechender deutscher Ausdruck finden lassen, etwa Wechsel-Folge = W-F; doch schien es, namentlich mit Rücksicht auf nichtdeutsche Leser, passend, die hier gewählte Abkürzung V-P beizubehalten.

worin

$$k_p = \frac{n-p+1}{n-p} \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; (2)$$

Der Kürze wegen soll $f^{(p)}(x)$ mit f_p bezeichnet werden.

Es soll nun untersucht werden, welche Veränderungen mit den V-P dieser Reihen vorgehen können, wenn x von einem niedrigeren Werthe zu einem höheren übergeht; zu bemerken ist, dass

$$2 - k_p = \frac{1}{k_{p+1}}, \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; (3)$$

und zuerst werde angenommen, dass zwei auf einander folgenden Glieder nicht gleichzeitig Null werden können.

Die Anzahl von V-P kann nur verändert werden, wenn ein Glied in einer der beiden Reihen durch Null hindurch geht; beispielsweise möge das mit f_p der Fall sein; die Veränderung findet dann statt bei den Gliedern

$$f_{p-1}; \; f^2_{p-1} - k_{p-1} f_{p-2} f_p,$$

$$f_p; \quad f^2_p - k_p f_{p-1} f_{p+1},$$

$$f_{p+1}; \; f^2_{p+1} - k_{p+1} f_p f_{p+2},$$

wo die Vorzeichen in der zweiten Reihe für $f_p = 0$

$$+ \pm +$$

sind.

Hier kann also nur V-P sein, wenn das mittlere Zeichen + ist, wenn also f_{p-1} und f_{p+1} verschiedene Vorzeichen haben; in diesem Falle sind in der ersten Reihe ein Zeichenwechsel und eine Zeichenfolge, so dass in den drei Paar Gliedern eine V-P ist, sowohl bevor als auch nachdem f_p Null geworden ist.

Dies gilt nicht, wenn f(x) durch Null hindurchgeht; in der ersten Reihe geht dann ein Zeichenwechsel in eine Zeichenfolge über, während die beiden ersten Glieder der zweiten Reihe beide positiv sind und also eine Zeichenfolge

bilden; hier wird also jedesmal eine V-P verloren, sobald x durch eine Wurzel der gegebenen Gleichung hindurchgeht, während keine Aenderung in der Anzahl von V-P hervorgebracht wird, sobald das zweite Glied der ersten Reihe Null wird.

Es bleibt noch zu untersuchen, ob die Anzahl der V-P dadurch verändert werden kann, dass die Glieder der zweiten Reihe durch Null hindurchgehen. Für die abgeleitete Function von $f^2_p - k_p f_{p-1} f_{p+1} = T_p$ erhält man

$$(2 - k_p) f_p f_{p+1} - k_p f_{p-1} f_{p+2},$$

aber für $T_p = 0$ ist

$$k_p f_{p-1} = \frac{f^2_p}{f_{p+1}}$$

und da $2 - k_p = \frac{1}{k_{p+1}}$, so kann die abgeleitete Function in der Form

$$\frac{1}{k_{p+1}} \frac{f_p}{f_{p+1}} (f^2_{p+1} - k_{p+1} f_p f_{p+2})$$

geschrieben werden, wo die Grösse in den Klammern eben das nächste Glied der Reihe, T_{p+1}, ist; man sieht also, dass das Glied T_p, wenn der Werth von x, für welchen es Null wird, einen hinreichend kleinen Zuwachs erhält, dasselbe Vorzeichen hat wie

$$\frac{f_p}{f_{p+1}} T_{p+1} h. \quad \ldots\ldots\ldots\ldots \quad (4)$$

T_p kann nur das Vorzeichen wechseln, wenn f_{p-1} und f_{p+1} dasselbe Vorzeichen haben; f_p muss also das entgegengesetzte Vorzeichen haben, wenn hier eine V-P ist. Die erste Reihe hat also die Zeichen

$$+ - + \text{ oder } - + -,$$

so dass $\frac{f_p}{f_{p+1}}$ negativ ist und T_p folglich dasselbe Vorzeichen erhält wie

$$- T_{p+1} h.$$

Für ein negatives h, das heisst, bevor T_p durch Null hindurchgeht, bilden deshalb T_p und T_{p+1} eine Zeichenfolge, welche für ein positives h in einen Zeichenwechsel übergeht; hier wird deshalb eine V-P verloren; wenn T_{p+1} dasselbe Vorzeichen hat wie T_{p-1}, wird auch zwischen T_{p-1} und T_p eine Zeichenfolge verloren, während im entgegengesetzten Falle eine gewonnen wird. *Man verliert also eine V-P für jede Wurzel von f(x), durch welche man hindurchgeht, und jedesmal zwei, wenn ein Glied der zweiten Reihe, indem es durch Null hindurchgeht, zwischen zwei Gliedern mit denselben Vorzeichen liegt, während gleichzeitig das entsprechende Glied der ersten Reihe mit dem vorangehenden und nachfolgenden Zeichenwechsel bildet.*

117. Es wurde vorausgesetzt, dass zwei Glieder nicht gleichzeitig Null werden können; werden zwei derselben gleichzeitig Null, so müssen die Coefficienten eine gewisse Bedingungsgleichung befriedigen, und man kann deshalb durch eine unendlich kleine Aenderung der Coefficienten diesen Fall auf den vorhergehenden zurückführen; diese Aenderung kann das Vorzeichen für irgend ein Glied der Reihe nicht verändern, sobald man nur dafür sorgt, dass durch die eingesetzten Grenzwerthe kein Glied gleich Null werden kann. Da nun die kleine Aenderung, wenn die Gleichung keine gleichen Wurzeln hat, die Anzahl der reellen Wurzeln innerhalb des Intervalles nicht verändern kann, giebt die Methode auch in diesem Falle eine obere Grenze für diese Anzahl.

Der Fall, wo ein Werth von x gleichzeitig f(x), $f'(x) \dots f^{(p)}(x)$ zum Verschwinden bringt, weil p + 1 Wurzeln gleich sind, muss besonders untersucht werden; man findet dann, wie bei dem Satze von Budan, dass die erste Reihe p Zeichenwechsel verliert; angenommen f_{p+1} sei positiv; die erste Reihe

$$f(x)\ f'(x) \dots f^{(p-1)}(x)\ f^{(p)}(x)\ f^{(p+1)}(x)$$

geht dann von

$$\dots + \ - \ +$$

über zu

$$\ldots + + +.$$

Die zweite Reihe erhält in den $p+1$ ersten Gliedern für $x-h$ lauter Zeichenfolgen; eines dieser Glieder sei

$$f^2_r - k_r f_{r-1} f_{r+2},$$

aber für $x=h$ ist

$$f_r = \pm f_{p+1} \frac{h^{p-r+1}}{(p-r+1)!}; \quad f_{r-1} = \mp f_{p+1} \frac{h^{p-r+2}}{(p-r+2)!};$$

$$f_{r+1} = \mp f_{p+1} \frac{h^{p-r}}{(p-r)!},$$

so dass das Vorzeichen des Gliedes dasselbe wird wie das von

$$\frac{1}{[(p-r+1)!]^2} - \frac{k_r}{(p-r+2)!\,(p-r)!}$$

oder von

$$\frac{p-r+2}{p-r+1} - \frac{n-r+1}{n-r};$$

der letzte Ausdruck ist aber, da $n > p$, positiv für jedes r. Die beiden Reihen beginnen also für $x-h$ mit p V-P, welche alle verloren werden, wenn man die p übereinstimmenden Wurzeln passirt. Der Satz gilt also auch für gleiche Wurzeln.

118. Was k_p betrifft, so wurde in der Entwicklung nur die Gleichung

$$2 - k_p = \frac{1}{k_{p+1}}$$

benutzt, indem vorausgesetzt wurde, dass k_p positiv sei; diese Bedingungen werden ebenso gut erfüllt, wenn man

$$k_p = \frac{m-p+1}{m-p}$$

setzt, worin $m > n$; wenn m ohne Grenze wächst, ist der Werth dieses Ausdrucks 1.

Beisp.

$$x^5 - 3x^4 + 2x^3 - 8x^2 + 3x - 25 = 0.$$
$$f'(x) = 5x^4 - 12x^3 + 6x^2 - 16x + 3;$$
$$f''(x) = 20x^3 - 36x^2 + 12x - 16;$$
$$f'''(x) = 60x^2 - 72x + 12;$$
$$f^{IV}(x) = 120x - 72;$$
$$f^{V}(x) = 120;$$

die Wurzeln liegen zwischen 0 und 4; für $x = 0$ erhält man

$$\begin{matrix} -25 & +3 & -16 & +12 & -72 & +120 \\ + & - & + & - & + & + \end{matrix},$$

wo die untere Reihe die Zeichen darstellt, welche den Gliedern T angehören; für $x = 4$ erhält man lauter Zeichenfolgen in der ersten Reihe und braucht deshalb nicht die Zeichen in der zweiten zu bestimmen; für $x = 0$ hat man eine V-P, für $x = 4$ keine; da die Gleichung keine negativen Wurzeln hat, hat sie also eine reelle und vier complexe Wurzeln.

119. In Vorstehendem wurden die verlorenen V-P betrachtet, um eine Grenze für die Anzahl der passirten Wurzeln zu finden; die Darstellung weicht dadurch etwas von derjenigen Sylvester's ab, welcher die Doppelzeichenfolgen (Doppelpermanenzen) P-P betrachtet; da beide Betrachtungen zusammengefasst werden müssen, soll untersucht werden, wie viele P-P gewonnen werden, wenn x von einem Werthe bis zu einem anderen wächst.

Wenn f(x) durch Null hindurchgeht, geht immer eine V-P in eine P-P über, so dass es hier gleichgültig ist, ob man die verlorene V-P oder die gewonnene P-P betrachtet; wenn ein anderes Glied der ersten Reihe, f_p, durch Null hindurchgeht, während die beiden einschliessenden Glieder verschiedene Zeichen haben, so sind die drei Glieder der zweiten Reihe positiv, so dass nur eine V-P und eine P-P ihren Platz wechseln; haben die beiden einschliessenden Glieder dasselbe Zeichen, bilden die drei Glieder der zweiten Reihe zwei Zeichen-

wechsel, so dass es auch in diesem Falle gleichgültig ist, ob man V-P oder P-P betrachtet.

Wenn T_p das Vorzeichen wechselt, haben f_{p-1} und f_{p+1} dasselbe Zeichen, so dass die erste Reihe zwei Zeichenwechsel oder zwei Zeichenfolgen hat. Falls nun T_{p-1} und T_{p+1} verschiedene Zeichen haben, findet nur eine Aenderung der Reihenfolge statt; es bleibt also nur der Fall zu betrachten übrig, wo T_{p-1} und T_{p+1} dasselbe Zeichen haben während T_p durch Null hindurchgeht.

Falls die erste Reihe zwei Zeichenfolgen hat, zeigt (4), dass T_p, nachdem es durch Null hindurchgegangen ist, dasselbe Zeichen wie T_{p+1} bekommt; hier gehen also zwei P-V in zwei P-P über.

Hat die erste Reihe zwei Zeichenwechsel, so zeigt (4), dass in der zweiten Reihe zwei Zeichenfolgen in zwei Zeichenwechsel übergehen; in diesem Falle gehen also zwei V-P in zwei V-V über; man kann deshalb den obenstehenden Satz durch folgenden ergänzen:

Wenn x wächst, wird jedesmal eine P-P gewonnen, sobald x durch eine Wurzel der gegebenen Gleichung hindurchgeht, und jedesmal zwei P-P, sobald ein Glied der zweiten Reihe verschwindet während die einschliessenden Glieder dasselbe Zeichen haben und die drei entsprechenden Glieder der ersten Reihe zwei Zeichenfolgen bilden.

120. Auf diese Weise hat man also zwei obere Grenzen für die Anzahl der reellen Wurzeln und kann zwischen diesen die niedrigste wählen. Dass dieses Bedeutung haben kann, sieht man am besten an dem obenstehenden Beispiel, wo man für $x = 0$ keine P-P erhält, während man für $x = 4$ deren 5 bekommt; hier würde also Sylvester's Satz 5 positive Wurzeln geben, während die Anwendung desselben in der veränderten Form 1 Wurzel giebt.

Um die ganze Anzahl der reellen Wurzeln einer Gleichung zu bestimmen, kann man $-\infty$ und $+\infty$ einsetzen; man muss deshalb in jedem Gliede der zweiten Reihe das Glied mit dem höchsten Exponenten bestimmen; ohne bei der hier-

für nöthigen Rechnung zu verweilen möge nur bemerkt werden, dass in T_p die beiden Glieder mit dem höchsten Exponenten fortfallen, so dass das Glied, welches benutzt werden soll, einen geraden Exponenten erhält; nach Unterdrückung eines positiven Factors wird der Coefficient desselben

$$a_1^2 - \frac{2n}{n-1} a_2, \quad \dots\dots\dots\dots\dots \quad (6)$$

wenn die Gleichung

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots = 0. \quad \dots\dots\dots \quad (7)$$

Falls nun

$$a_1^2 > \frac{2n}{n-1} a_2,$$

würden die Vorzeichen der zweiten Reihe alle $+$ werden, sowohl für $z = -\infty$ als auch für $x = +\infty$; ist

$$a_1^2 < \frac{2n}{n-1} a_2,$$

werden alle Vorzeichen —, mit Ausnahme des ersten und letzten, welche $+$ sind; im ersten Falle gewinnt man also n P-P, oder man verliert n V-P, und die Methode gewährt also keinerlei Aufschluss; im zweiten Falle zeigt die Methode, dass die Gleichung zwei complexe Wurzeln hat. Nur zwei solcher Wurzeln hönnen deshalb durch einen der Sätze nachgewiesen werden; um ein besseres Resultat zu erhalten, muss man das Intervall in kleinere theilen, und für jedes von diesen denjenigen der beiden Sätze benutzen, welcher die niedrigste Grenze für die Anzahl der reellen Wurzeln giebt.

Für $x = 0$ erhält man aus (7)

$$f = a_n, \ f_1 = a_{n-1}, \ f_2 = 2a_{n-2} \dots f_p = p!\, a_{n-p} \dots;$$

hieraus folgt dann

$$T_p = (p!)^2 a^2_{n-p} - \frac{n-p+1}{n-p} (p-1)!\,(p+1)!\, a_{n-p-1}\, a_{n-p+1},$$

oder, wenn der positive Factor $(p!)^2$ entfernt wird,

$$T_p = a^2_{n-p} - \frac{p+1}{p} \cdot \frac{n-p+1}{n-p} a_{n-p-1} a_{n-p+1},$$

gültig für alle Glieder mit Ausnahme des ersten und letzten, welche positiv sind.

Es war nur dieser Fall, welchen Newton betrachtete, und für welchen er seinen Satz ohne Beweis gab; die beiden Reihen werden dann, wenn man die Glieder in umgekehrter Reihenfolge nimmt und positive Factoren auslässt

$$\begin{array}{llll} +, & a_1, & a_2, & a_3, \ldots \\ +, & a_1^2 - \frac{2n}{n-1} a_2, & a_2^2 - \frac{3(n-1)}{2(n-2)} a_1 a_3, & a_3^2 - \frac{4(n-2)}{3(n-3)} a_2 a_4 \ldots \end{array}$$

Angenommen, hier wären q P-P. Für $x = -\infty$ giebt es keine P-P; *also hat die Gleichung nicht mehr negative Wurzeln, als die beiden Reihen P-P haben (q); ferner nehme man an, dass die beiden Reihen* q_1 *V-P hätten;* für $x = \infty$ giebt es keine V-P; *also hat die Gleichung nicht mehr positive Wurzeln, als die beiden Reihen V-P haben* (q_1). Hieraus kann man wiederum schliessen, *dass die Gleichung wenigstens ebenso viele complexe Wurzeln hat, wie die zweite Reihe Zeichenwechsel* $(n - q - q_1)$.

Indem Newton auf diese Weise P-P für ein negatives x, dagegen V-P für ein positives x benutzt, erhält er in der Regel eine genauere Bestimmung der Anzahl der reellen Wurzeln als Sylvester; bei dem oben angeführten Beispiel zeigt beispielsweise der Satz von Newton, dass hier nur 1 positive Wurzel vorhanden ist, während man, wenn man Sylvester folgend nur P-P benutzt, 5 solcher Wurzeln bekommt, dieselbe Anzahl, welche der Satz von Descartes geben würde.

Erweiterung des Satzes von Descartes.

121. In Folgendem soll nun gezeigt werden, wie man durch eine von der obenstehenden ganz verschiedene Betrachtung zu einer Bestimmung der Anzahl der Wurzeln gelangen kann, welche sehr genau mit der vorigen übereinstimmt; nur in einzelnen Fällen steht sie etwas vor derselben zurück, während sie oft besser ist und mit grosser Leichtigkeit angewendet wird.

Bei dem Beweise des Satzes von Descartes wurde früher gezeigt, dass man durch Einführung einer positiven Wurzel in die Gleichung die Anzahl der Zeichenwechsel um wenigstens 1 vermehrt. Falls mehr als 1 Zeichenwechsel durch die Multiplication eingeführt wird, muss die Anzahl der Zeichenfolgen vermindert werden, und man erhält so eine genauere Bestimmung der Anzahl der negativen Wurzeln, da diese durch Einführung der positiven Wurzel nicht verändert wird.

Wenn der erste negative Coefficient der Gleichung $-a_p$ ist, wird die durch Multiplication mit $x-\alpha$ erhaltene neue Gleichung, wenn man die Glieder derselben einzeln unter die Glieder der gegebenen schreibt, an derselben Stelle ein negatives Glied erhalten; dann würde es darauf ankommen, ob man α so wählen könnte, dass einige der vorhergehenden Zeichenfolgen in Zeichenwechsel übergehen würden; man erhält nun durch Multiplication von

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} \ldots + a_{p-1} x^{n-p+1} - a_p x^{n-p} \quad \ldots \quad (1)$$

mit $x-\alpha$

$$x^{n+1} + (a_1-\alpha) x^n \ldots + (a_{p-1} - \alpha a_{p-2}) x^{n-p+2} - m x^{n-p+1}, \quad (2)$$

wo m positiv ist; nun setze man

$$\frac{a_r}{a_{r-1}} = k_r. \quad \ldots \ldots \ldots \ldots \quad (3)$$

Die Zeichen in der neuen Gleichung werden dann dieselben wie die für

$$1,\ k_1 - \alpha,\ k_2 - \alpha,\ \ldots k_{p-1} - \alpha,\ - \ldots$$

Der erste positive Coefficient nach $-a_p$ sei a_q, der erste dann folgende negative sei $-a_r$ u. s. w.; für diese Theile der Reihe erhält man dann dieselben Zeichen wie für

$$\begin{array}{l} -,\ \alpha - k_{p+1},\ \alpha - k_{p+2},\ \ldots \alpha - k_{q-1}, \\ +,\ k_{q+1} - \alpha,\ k_{q+2} - \alpha,\ \ldots k_{r-1} - \alpha, \\ -,\ \alpha - k_{r+1},\ \alpha - k_{r+2},\ \ldots \alpha - k_{s-1} \ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}$$

Falls nun die in jeder Gruppe vorkommenden Quotienten k an Grösse abnehmen, ist es gleichgültig, welchen Werth man α beilegt; man kann dann die Zeichenwechsel verschieben, aber nicht ihre Anzahl vermehren; im entgegengesetzten Falle muss immer ein Werth von α, welcher zwischen dem grössten und kleinsten k einer Gruppe liegt, die Anzahl der Zeichenfolgen vermindern; man bestimmt leicht den Werth von α, für welchen die grösstmögliche Anzahl Zeichenfolgen in Zeichenwechsel übergeht; die neue Gleichung kann dann auf dieselbe Weise behandelt werden und so fährt man fort, bis man zu einer Gleichung gelangt ist, in der die Quotienten k in jeder Gruppe abnehmend sind. Die Grenze für die Anzahl der positiven Wurzeln wird dann auf dieselbe Weise bestimmt, nachdem x mit $-x$ vertauscht worden ist.

Beisp.

$$x^8 + x^7 + 4x^6 + 8x^5 - x^4 - 7x^3 - 22x^2 + 152x - 450 = 0.$$

$$1 \qquad 4 \qquad 2 \qquad\qquad \frac{22}{7}$$

Die Zahlen geben die Werthe von k an; setzt man $\alpha = 3$, so gehen die ersten drei Zeichenfolgen in Zeichenwechsel über, und man erhält dann nur Zeichenfolgen in

$$-4x^6 - 25x^5 - 4x^4 - x^3 + \ldots$$

$$\frac{25}{4} \qquad \frac{4}{25} \qquad \frac{1}{4} \ \ldots\ldots,$$

woraus die neue Gruppe von Zeichen

$$-,\ a-\frac{25}{4},\ a-\frac{4}{25},\ a-\frac{1}{4},\ +\ldots,$$

so dass man für

$$\frac{1}{4}>a>\frac{4}{25}$$

nur 1 Zeichenfolge erhält; die Gleichung hat also nur 1 negative Wurzel.

Der Satz von Newton giebt

$$\begin{array}{ccccccccc} + & + & + & + & - & - & - & + & - \\ + & - & + & + & + & + & + & + & +, \end{array}$$

also drei P - P.

Um die Anzahl der positiven Wurzeln zu finden, wird x mit $-x$ vertauscht; man erhält dann

$$x^8-x^7+4x^6-8x^5-x^4+7x^3-22x^2-152x-450=0.$$

Bei den letzten Zeichenfolgen ist der Quotient abnehmend, so dass man durch eine Multiplication diese Zeichenfolgen nicht entfernen kann; das Resultat ist also, dass die Gleichung 1 oder 3 positive Wurzeln enthält, ebenso wie es durch den Satz von Newton gefunden wird.

Zweites Kapitel.

Berechnung der Wurzeln in numerischen Gleichungen.

Bestimmung der rationalen Wurzeln.

122. Eine Gleichung mit gebrochenen Coefficienten kann, wie früher in 42 gezeigt worden, immer in eine andere umgewandelt werden, deren Coefficienten ganze Zahlen sind und deren erstes Glied den Coefficienten 1 hat. In der Folge wird diese Umwandlung immer als geschehen vorausgesetzt.

Eine Gleichung, deren erstes Glied den Coefficienten 1 hat, während die übrigen Coefficienten ganze Zahlen sind, kann keine rationale Wurzel haben, welche gebrochen ist.

Die Gleichung sei

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n = 0. \quad \ldots\ldots\ldots (1)$$

Wenn der irreductible Bruch $\frac{p}{q}$ eine Wurzel dieser Gleichung ist, muss man haben

$$\frac{p^n}{q^n} = -\left(a_1 \frac{p^{n-1}}{q^{n-1}} + a_2 \frac{p^{n-2}}{q^{n-2}} + \ldots + a_n\right)$$

oder

$$\frac{p^n}{q} = -(a_1 p^{n-1} + a_2 p^{n-2} q + \ldots + a_n q^{n-1}),$$

aber das ist unmöglich, da der Bruch auf der linken Seite des Gleichheitszeichens irreductibel ist, während sich auf der rechten Seiten eine ganze Zahl befindet.

123. Soll man also die rationalen Wurzeln einer Gleichung bestimmen, so kann man derselben auf die früher angegebene Weise ganze Coefficienten verschaffen; die rationalen Wurzeln der Gleichung müssen dann ganze Zahlen sein; wie man diese durch einige Versuche bestimmen kann, wird in Folgendem gezeigt werden.

Die Gleichung (1) sei die gegebene und t sei die ganze Zahl, welche eine Wurzel derselben ist; dann hat man

$$t^n + a_1 t^{n-1} + a_2 t^{n-2} + \ldots + a_{n-2} t^2 + a_{n-1} t + a_n = 0,$$

woraus hervorgeht, dass t ein Factor von a_n sein muss; man mache dann die Probe mit den verschiedenen Factoren von a_n, sowohl positiv wie negativ genommen; wenn keiner von diesen die Gleichung befriedigt, so hat dieselbe keine rationale Wurzel.

Um mit dem Factor t die Probe zu machen, dividire man die obenstehende Gleichung durch denselben, und erhält dann, wenn man

$$a_n = t\, q_{n-1}$$

setzt,

$$t^{n-1} + a_1 t^{n-2} + a_2 t^{n-3} + \ldots a_{n-1} + q_{n-1} = 0,$$

woraus folgt, dass $a_{n-1} + q_{n-1}$ durch t theilbar sein muss; bezeichnet man den Quotienten mit q_{n-2}, so sieht man auf dieselbe Weise, dass $a_{n-2} + q_{n-2}$ durch t theilbar sein muss; zuletzt erhält man dann

$$1 + q_0 = 0.$$

Sobald während des Verlaufs der Rechnung einer der Quotienten q gebrochen wird, kann der Werth, mit welchem man die Probe macht, keine Wurzel sein; sind dagegen alle Quotienten ganze Zahlen, und schliesst man mit $q_0 = -1$, so hat man eine Wurzel gefunden, und bei der Art und Weise, wie hier die Rechnung angeordnet ist, ist zugleich der der Wurzel entsprechende Factor entfernt worden; der Quotient wird nämlich

$$x^{n-1} - q_1 x^{n-2} - q_2 x^{n-3} \dots - q_{n-1}$$

sein, da diese Grösse durch Multiplication mit $x - t$

$$x^n - (q_1 + t) x^{n-1} \dots + (t q_{p-1} - q_p) x^{n-p} \dots + t q_{n-1}$$

wird; es wurde aber

$$a_p + q_p = t q_{p-1}$$

gesetzt, so dass

$$t q_{p-1} - q_p = a_p.$$

Wie man am besten bei der Rechnung zu verfahren hat, wird durch das folgende Beispiel ersichtlich.

Beisp.

$$x^5 - 47 x^4 + 423 x^3 - 140 x^2 + 1243 x + 420 = 0.$$

Man mache z. B. die Probe mit $x = 3$ und erhält

$$\begin{array}{rrr} \dots\dots - 140 x^2 & + 1213 x & + 420. \\ 451 & 140 & \\ \hline 311 & 1353 & \end{array}$$

3 geht nicht auf in 311 und kann deshalb keine Wurzel sein; versucht man mit 12, so erhält man

$$\begin{array}{rrrrrr} 1 & -47 & 423 & -140 & 1213 & 420. \\ -1 & 35 & -3 & 104 & 35 & \\ \hline 0 & -12 & 420 & -36 & 1248 & \end{array}$$

Man sieht hieraus, dass 12 eine Wurzel ist und dass die Division durch $x - 12$

$$x^4 - 35x^3 + 3x^2 - 104x - 35 = 0.$$

giebt.

Die Probe mit 35 giebt

$$\begin{array}{rrrrr} 1 & -35 & 3 & -104 & -35, \\ -1 & 0 & -3 & -1 & \\ \hline & -35 & 0 & -105 & \end{array}$$

und somit gelangt man zu der Gleichung

$$x^3 + 3x + 1 = 0,$$

welche keine rationalen Wurzeln hat.

Um das Probiren auf ein möglichst geringes Mass einzuschränken, muss man erst die Grenzen der Wurzeln bestimmen; man vermeidet dadurch die Factoren von a_n, welche ausserhalb der Grenzen liegen; ferner ist zu beachten, dass, wenn $f(x)$ theilbar ist durch $x - t$, auch die Quotienten

$$\frac{f(1)}{t-1}, \frac{f(-1)}{t+1}, \frac{f(2)}{t-2}, \frac{f(-2)}{t+2}$$

ganze Zahlen werden müssen; die kleineren Factoren -1, $+1\ldots$ berücksichtigt man durch Einsetzen in die Gleichung; dadurch erhält man bei dem obenstehenden Beispiel

$$f(-1) = -1404; \; f(1) = 1870.$$

Man hat also nicht nöthig, mit dem Factor 10 die Probe zu machen, da 1404 nicht theilbar ist durch 11; dagegen muss man -10 versuchen, da 1404 durch 9 und 1870 durch 11 theilbar ist; hat man zugleich

$$f(2) = 4940$$

berechnet, welches nicht theilbar ist durch 12, so sieht man, dass -10 keine Wurzel sein kann.

Interpolation.

124. Nachdem man eine Wurzel abgesondert hat, ist es nothwendig die Grenzen derselben einander möglichst zu nähern, ehe man die eigentliche Berechnung in Angriff nimmt; dies kann dadurch geschehen, dass man Werthe von x, welche zwischen den beiden Grenzen liegen, in f(x) einsetzt, da man dann aus dem Vorzeichen von f(x) schliessen kann, innerhalb welches der beiden Intervalle, worin das erste Intervall getheilt ist, die Wurzel belegen ist. Auf diese Weise kann man fortfahren bis man die Grenzen einander so nahe gebracht hat, wie man wünscht; aber, obgleich diese Methode einfach genug erscheint, wird man dieselbe in der Praxis sehr beschwerlich finden; man schlägt deshalb einen anderen Weg ein, der leichter zum Ziele führt.

125. *Differenzen einer Function.* Es seien

$$u_0, u_1, u_2 \ldots$$

eine Reihe von Grössen, die durch ein oder das andere Gesetz bestimmt werden; dann setzt man

$$u_{n+1} - u_n = \Delta u_n \ldots\ldots\ldots\ldots\ldots (1)$$

und nennt diese Grösse *die erste Differenz* von u_n; auf ähnliche Weise werden zweite, dritte u. s. w. Differenzen gebildet, nämlich

$$\Delta u_{n+1} - \Delta u_n = \Delta^2 u_n, \ldots\ldots\ldots\ldots\ldots (2)$$
$$\Delta^2 u_{n+1} - \Delta^2 u_n = \Delta^3 u_n \text{ u. s. w.}$$

Hieraus erhält man

$$\begin{aligned}\Delta^2 u_n &= \Delta u_{n+1} - \Delta u_n \\ &= u_{n+2} - u_{n+1} \\ &\qquad - u_{n+1} + u_n \\ &= u_{n+2} - 2u_{n+1} + u_n,\end{aligned}$$

$$\begin{aligned}\Delta^3 u_n &= \Delta (u_{n+2} - 2 u_{n+1} + u_n) \\ &= u_{n+3} - 2 u_{n+2} + u_{n+1} \\ &\quad\quad - u_{n+2} + 2 u_{n+1} - u_n \\ &= u_{n+3} - 3 u_{n+2} + 3 u_{n+1} - u_n.\end{aligned}$$

Wie man sieht, werden die Coefficienten auf dieselbe Weise gebildet wie die Coefficienten beim Potenziren von $a - b$; man hat deshalb allgemein

$$\Delta^p u_n = u_{n+p} - \frac{p}{1} u_{n+p-1} + \frac{p(p-1)}{1.2} u_{n+p-2} \cdots + (-1)^p u_n. \quad (3)$$

Man sieht hieraus, wie jede Differenz durch die Glieder der Reihe ausgedrückt werden kann; umgekehrt kann jedes Glied durch das erste Glied und dessen Differenzen ausgedrückt werden; man hat nämlich

$$u_1 = u_0 + \Delta u_0.$$

woraus

$$\Delta u_1 = \Delta u_0 + \Delta^2 u_0,$$

aber

$$u_2 = u_1 + \Delta u_1,$$

also

$$u_2 = u_0 + 2 \Delta u_0 + \Delta^2 u_0;$$

ferner ist

$$\begin{aligned}u_3 &= u_2 + \Delta u_2 \\ &= u_0 + 2 \Delta u_0 + \Delta^2 u_0 \\ &\quad\quad + \Delta u_0 + 2 \Delta^2 u_0 + \Delta^3 u_0 \\ &= u_0 + 3 \Delta u_0 + 3 \Delta^2 u_0 + \Delta^3 u_0.\end{aligned}$$

Hier sieht man, dass die Coefficienten wie beim Potenziren von $a + b$ gebildet werden; man hat also allgemein

$$u_p = u_0 + \frac{p}{1} \Delta u_0 + \frac{p(p-1)}{1.2} \Delta^2 u_0 + \ldots + \Delta^p u_0. \quad \ldots \quad (4)$$

126. *Differenzen ganzer Functionen.* Sei

$$u = f(x) = a_0 x^n + a_1 x^{n-1} + \quad \ldots\ldots\ldots\ldots \quad (5)$$

eine ganze Function von x, in welcher x nach und nach die Werthe

$$x_0, x_0 + h, x_0 + 2h, \ldots x_0 + nh$$

beigelegt werden; die entsprechenden Werthe der Function mögen durch

$$u_0, u_1, u_2 \ldots u_n$$

bezeichnet werden.

Dann hat man

$$\triangle u = f(x + h) - f(x) = n a_0 x^{n-1} h + \ldots, \ldots\ldots (6)$$

woraus hervorgeht, dass $\triangle u$ um einen Grad niedriger ist als u; $\triangle^2 u$ ist dann um zwei Grade niedriger und hat als erstes Glied $n(n-1) a_0 x^{n-2} h^2$ u. s. w.; hieraus folgt, dass, *wenn eine Function vom n^{ten} Grade ist, ihre n^{ten} Differenzen constant sein werden,* nämlich

$$\triangle^n u = n!\, a_0 h^n. \ldots\ldots\ldots\ldots (7)$$

Noch höhere Differenzen werden alle Null. *Eine Reihe, deren n^{te} Differenzen constant sind, heisst eine Differenzenreihe n^{ter} Ordnung.*

Beisp.

$$f(x) = x^4;\ h = 1;\ x_0 = 1.$$

u_0 u_1 u_2 u_3 u_4 ...
1 16 81 256 625 ...
$\triangle u_0$ $\triangle u_1$ $\triangle u_2$ $\triangle u_3$ ...
15 65 175 369 ...
$\triangle^2 u_0$ $\triangle^2 u_1$ $\triangle^2 u_2$ ...
50 110 194 ...
$\triangle^3 u_0$ $\triangle^3 u_1$ ...
60 84 ...
$\triangle^4 u_0$ ...
24 ...

Man hat nun z. B. zufolge (4) und (3)

$$u_5 = 1 + 5.15 + 10.50 + 10.60 + 5.24 = 1296 = 6^4$$
$$\triangle^4 u_0 = 1 - 4.16 + 6.81 - 4.256 + 625 = 24.$$

127. *Substitution aequidistanter Werthe von x in $f(x)$.* Wenn man eine Reihe äquidistanter Werthe von x in f(x) einsetzen soll, hat man nur nöthig, n auf einander folgende Werthe einzusetzen; mit Hülfe dieser kann man durch eine Reihe Subtractionen die Differenzen finden und man kann dann durch einfache Additionen die Werthe der Function für die übrigen Glieder der Reihe bestimmen.

Die gegebene Function sei z. B.

$$u = x^3 - 5x + 6,$$

welche für $x = 1, 2, 3 \ldots$ berechnet werden soll; dann hat man, wenn $x_0 = 1$, für

$$x = 1,\ x = 2 \text{ und } x = 3$$

u	$\triangle u$	$\triangle^2 u$	$\triangle^3 u$
2			
	2		
4		12	6.
	14		
18			

Wie man weiss, ist 6 die letzte Differenz. Die Reihe für $\triangle^2 u$ kann also nach oben und nach unten ergänzt werden, da zwei auf einander folgende Glieder die Differenz 6 haben; nun kann die vorhergehende Reihe gebildet werden, da man die Differenz für je zwei Glieder kennt u. s. w.; man erhält also für $\triangle^2 u$

$$6,\ 12,\ 18,$$

und darauf für $\triangle u$

$$-4,\ 2,\ 14,\ 32,$$

wodurch endlich die Reihe von u

$$6,\ 2,\ 4,\ 18,\ 50$$

wird, so dass man

$$f(0) = 6;\ f(4) = 50$$

gefunden hat.

128. *Bestimmung von $f(x)$ mit Hülfe ihrer Werthe für $n+1$ aequidistante Werthe von x.* Schreibt man die Formel (4) in der Form

$$u_p = u_0 + \frac{p}{1} \Delta u_0 + \frac{p(p-1)}{1.2} \Delta^2 u_0 + \dots$$
$$\dots + \frac{p(p-1)\dots(p-n+1)}{1.2.3\dots n} \Delta^n u_0,$$

und setzt

$$p = \frac{x - x_0}{h},$$

während man für u_0, Δu_0, $\Delta^2 u_0 \dots$ die durch $u = f(x)$ bestimmten Ausdrücke nimmt, so erhält man

$$u_{\frac{x-x_0}{h}} = u_0 + \frac{x-x_0}{1} \frac{\Delta u_0}{h} + \frac{(x-x_0)(x-x_0-h)}{1.2} \frac{\Delta^2 u_0}{h^2} + \dots$$
$$+ \frac{(x-x_0)(x-x_0-h)\dots(x-x_0-[n-1]h)}{1.2\dots n} \frac{\Delta^n u_0}{h^n}. \quad \dots (8)$$

Da die Formel für alle ganzen Werthe von p gilt, gilt sie auch für

$$x = x_0, \; x = x_0 + h, \; x = x_0 + 2h, \; \dots x = x_0 + nh.$$

Bezeichnet man den Ausdruck auf der rechten Seite des Gleichheitszeichens mit $F(x)$, sieht man also, dass der Gleichung

$$f(x) = F(x)$$

durch $n+1$ Werthe von x Genüge geleistet wird; da nun diese Gleichung höchstens vom n^{ten} Grade ist, muss dieselbe identisch sein, und man hat also $f(x)$ mit Hülfe der $n+1$ gegebenen Werthe gefunden.

Beisp. Es soll eine Function dritten Grades bestimmt werden, welche für $x=1$, $x=2$, $x=3$, $x=4$ beziehungsweise die Werthe 5, 11, 13 und 21 hat.

Man hat

$$\begin{array}{ccccccc} 5 & & 11 & & 13 & & 21 \\ & 6 & & 2 & & 8 & \\ & & -4 & & +6 & & \\ & & & 10 & & & \end{array}$$

also

$$u_0 = 5,\ \Delta u_0 = 6,\ \Delta^2 u_0 = -4,\ \Delta^3 u_0 = 10,\ h = 1;$$

folglich ist

$$f(x) = 5 + 6(x-1) - 2(x-1)(x-2) + \frac{5}{3}(x-1)(x-2)(x-3).$$

129. *Interpolation.* Mit Hülfe der entwickelten Sätze kann man nun die früher gestellte Aufgabe lösen, die darin bestand, die Werthe einer Function für Werthe von x zu berechnen, welche zwischen den früher benutzten liegen. Gewöhnlich theilt man h in eine gewisse Anzahl gleich grosser Theile; man setzt dann beispielsweise

$$h = q h_1,$$

und erhält dann die $x = x_0 + m h_1$ entsprechenden Werthe der Function mit Hülfe von (8), wonach

$$f(x_0 + m h_1) = u_0 + A_1 \Delta u_0 + A_2 \Delta^2 u_0 + \ldots + A_n \Delta^n u_0,$$

worin

$$A_k = \frac{m(m-q)(m-2q)\ldots(m-[k-1]q)}{1.2.3\ldots k.q^k} \quad \ldots\ldots (9)$$

Setzt man z. B. $h = 1$, $h_1 = \frac{1}{10}$, so erhält man

$$A_k = \frac{m(m-10)(m-20)\ldots(m-10[k-1])}{1.2.3\ldots k.10^k} \quad \ldots\ldots (10)$$

Um $f(x_0 + m h_1)$ zu berechnen setzt man indessen nicht die Werthe von m in A_k ein, sondern man berechnet die Differenzen der Function, welche dem neuen Intervall entsprechen; man hat dann, wenn man diese mit δ bezeichnet,

$$\begin{aligned}
u_0 &= u_0 \\
\delta u_0 &= \delta A_1 \Delta u_0 + \delta A_2 \Delta^2 u_0 + \delta A_3 \Delta^3 u_0 + \ldots \\
\delta^2 u_0 &= \qquad\qquad \delta^2 A_2 \Delta^2 u_0 + \delta^2 A_3 \Delta^3 u_0 + \ldots \\
\delta^3 u_0 &= \qquad\qquad\qquad\qquad \delta^3 A_3 \Delta^3 u_0 + \ldots,
\end{aligned}$$

da

$$\delta u_0 = 0,\ \delta^2 A_1 = 0,\ \delta^3 A_2 = \delta^3 A_1 = 0 \text{ u. s. w.},$$

weil u_0, A_1, $A_2 \ldots$ mit Bezug auf m beziehungsweise von den Graden 0, 1, 2 … sind. In den Ausdrücken auf der

rechten Seite muss man den u_0 entsprechenden Werth nehmen, also $m = 0$; man hat nun für $q = 10$

$$A_1 = \frac{m}{10}; \ \delta A_1 = 0{,}1$$

$$A_2 = \frac{m(m-10)}{1.2.10^2}; \ \delta A_2 = -0{,}045, \ \delta^2 A_2 = 0{,}01$$

$$A_3 = \frac{m(m-10)(m-20)}{1.2.3.10^3}; \ \delta A_3 = 0{,}0285, \ \delta^2 A_3 = -0{,}009, \ \delta^3 A_3 = 0{,}001.$$

In der oben bestimmten Function war

$$u_1 = 5, \ \Delta u_0 = 6, \ \Delta^2 u_0 = -4, \ \Delta^3 u_0 = 10,$$

also

$$\delta u_0 = 6.0{,}1 + 4.0{,}045 + 10.0{,}0285 = 1{,}065,$$
$$\delta^2 u_0 = -4.0{,}01 - 10.0{,}009 = -0{,}13,$$
$$\delta^3 u_0 = 10.0{,}001 = 0{,}01.$$

Man berechnet dann die Werthe der Function für

$$x = 1{,}1, \ x = 1{,}2 \ldots x = 1{,}9$$

indem man folgende Tabelle entwirft:

x	u	δu	$\delta^2 u$	$\delta^3 u$
1,0	5,000	1,065	— 0,13	0,01
1,1	6,065	0,935	— 0,12	0,01
1,2	7,000	0,815	— 0,11	0,01
1,3	7,815	0,705	— 0,10	0,01
1,4	8,520	0,605	— 0,09	0,01
1,5	9,125	0,515	— 0,08	0,01
1,6	9,640	0,435	— 0,07	0,01
1,7	10,075	0,365	— 0,06	0,01
1,8	10,440	0,305	— 0,05	
1,9	10,745	0,255		
2,0	11,000			

Wenn man diese Tabelle nach oben vervollständigt, findet man, dass die Function für einen Werth von x, der zwischen 0,6 und 0,7 liegt, gleich Null wird.

Newton's Näherungs-Methode.

130. Angenommen, eine Wurzel der Gleichung $f(x) = 0$ sei zwischen zwei nahe beisammen liegenden Grenzen a und b, wo $a < b$, abgesondert. Wenn man $x = a$ setzt, wird man einen Fehler x_1 begehen, welcher bestimmt wird durch die Gleichung

$$f(a + x_1) = 0 \text{ oder } 0 = f(a) + f'(a) x_1 + \frac{1}{2} f''(a) x_1^2 + \dots$$

Da x_1 hier sehr klein ist, werden im Allgemeinen die Glieder, welche x_1^2, x_1^3 u. s. w. enthalten, klein sein im Verhältniss zu dem Gliede, welches x_1 enthält. Newton vernachlässigt deshalb die Glieder, welche höhere Potenzen von x_1 enthalten, und setzt

$$0 = f(a) + f'(a) x_1 \text{ also } x_1 = -\frac{f(a)}{f'(a)}$$

oder

$$x = a - \frac{f(a)}{f'(a)}; \quad \dots\dots\dots\dots\dots \quad (1)$$

man erhält dadurch einen neuen Näherungswerth, der in der Regel genauer sein wird als der erste; aus diesem wird ein neuer auf dieselbe Weise abgeleitet u. s. w.

Beisp.

$$x^3 - 2x - 5 = 0.$$

Die Gleichung hat eine Wurzel zwischen 2 und 2,1. Man hat

$$f(x) = x^3 - 2x - 5$$
$$f'(x) = 3x^2 - 2.$$

Setzt man $a = 2$, erhält man

$$x = 2 - \frac{-1}{10} = 2{,}1;$$

nun ist

$$f(2{,}1) = 0{,}061; \; f'(2{,}1) = 11{,}23,$$

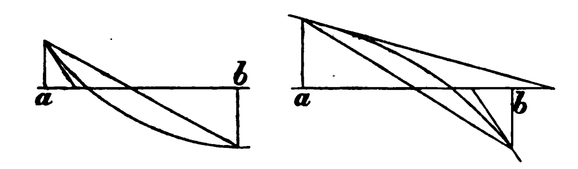
woraus

$$x = 2,1 - 0,0054 = 2,0946;$$

hieraus erhält man wieder

$$x = 2,0946 - \frac{f(2,0946)}{f'(2,0946)} = 2,0946 - 0,000048517 = 2,094551483.$$

131. *Mängel der Methode.* Newton's Methode wird mit ziemlicher Leichtigkeit angewendet, aber sie kann nicht immer mit Sicherheit benutzt werden, da es sich ereignen kann, dass die hinzugefügte Verbesserung den Fehler grösser anstatt kleiner macht; man übersieht die Verhältnisse leicht mit Hülfe der früher angewendeten geometrischen Betrachtung; man soll den Durchschnittspunkt der Curve $y = f(x)$ mit der



Axe bestimmen und hat einen Punkt mit der Abscisse a gefunden, welcher in der Nähe des Durchschnittspunktes liegt; Newton's Methode stimmt nun mit der überein, wonach man statt der Curve die Tangente an den Punkt nimmt, dessen Abscisse a ist; diese Tangente hat nämlich die Gleichung

$$y - f(a) = f'(a)(x - a),$$

und der Durchschnittspunkt derselben mit der Axe wird bestimmt durch $y = 0$, woraus

$$x = a - \frac{f(a)}{f'(a)},$$

übereinstimmend mit Newton's Formel; man sieht indessen leicht, dass der Durchschnittspunkt der Tangente mit der Axe weiter von dem gesuchten Durchschnittspunkt entfernt

Geht man von diesen Grenzwerthen aus, so erhält man wie oben

$$a_2 = 2{,}094551483$$

und ausserdem

$$b_2 = 2{,}0946 - 0{,}000048528 = 2{,}094551472.$$

Methode von Lagrange.

133. Nachdem eine Wurzel zwischen zwei auf einander folgenden ganzen Zahlen a und a + 1 abgesondert ist, setze man

$$x = a + \frac{1}{x_1}$$

und bilde die Gleichung in x_1. Falls die gesuchte Wurzel negativ ist, vertausche man erst x mit — x.

Wenn nun die gegebene Gleichung nur eine Wurzel zwischen a und a + 1 hat, erhält die transformirte Gleichung nur eine positive Wurzel grösser als 1; diese wird zwischen zwei ganzen Zahlen b und b + 1 abgesondert, und darauf setze man

$$x_1 = b + \frac{1}{x_2}.$$

Durch wiederholte Anwendung dieser Methode erhält man die gesuchte Wurzel ausgedrückt durch den Kettenbruch

$$x = a + \cfrac{1}{b + \cfrac{1}{\ddots}}$$

Hat die gegebene Gleichung mehrere Wurzeln zwischen a und a + 1, so bekommt die transformirte Gleichung mehrere Wurzeln grösser als 1; man muss dann mit jeder von diesen auf dieselbe Weise wie oben weiter rechnen.

Beisp.

$$f(x) = x^3 - 2x - 5 = 0.$$

Man setze

$$x = 2 + \frac{1}{x_1}$$

und erhält, da

$$f(x) = f(2) + f'(2)\frac{1}{x_1} + \frac{1}{2} f''(2)\frac{1}{x_1^2} + \frac{1}{x_1^3}$$
$$= -1 + 10 \cdot \frac{1}{x_1} + 6 \cdot \frac{1}{x_1^2} + \frac{1}{x_1^3},$$

die transformirte Gleichung

$$f_1(x_1) = x_1^3 - 10x_1^2 - 6x_1 - 1 = 0.$$

Die positive Wurzel dieser Gleichung liegt zwisshen 10 und 11; man setze also

$$x_1 = 10 + \frac{1}{x_2}.$$

Nun ist

$$\begin{aligned} f_1(x) &= x^3 - 10x^2 - 6x - 1 & f_1(10) &= -61 \\ f_1'(x) &= 3x^2 - 20x - 6 & f_1'(10) &= +94 \\ \frac{1}{1.2} f_1''(x) &= 3x - 10 & \frac{1}{2} f_1''(10) &= +20, \end{aligned}$$

so dass die neu transformirte Gleichung

$$-61x_2^3 + 94x_2^2 + 20x_2 + 1 = 0$$

wird, deren positive Wurzel zwischen 1 und 2 belegen ist; nunmehr liegt also die gesuchte Wurzel zwischen den beiden Kettenbrüchen

$$2 + \cfrac{1}{10 + \cfrac{1}{1}} \text{ und } 2 + \cfrac{1}{10 + \cfrac{1}{2}}$$

oder zwischen

$$\frac{23}{11} \text{ und } \frac{44}{21}.$$

134. Die Methode führt im Allgemeinen nur mit Beschwerlichkeit zu einem einigermassen genauen Resultat; Lagrange hat gezeigt, wie man den letzten Theil der Rechnung abkürzen kann; da man aber selbst mit diesen Veränderungen die Methode nicht mit Vortheil anwenden kann, so können dieselben füglich übergangen werden; dagegen soll gezeigt werden, wie die Methode oft auf Grund der besonderen Form der transformirten Gleichungen mit Vortheil mit einer anderen verbunden werden kann.

Gegeben sei die oben gefundene Gleichung

$$f_1(x_1) = x_1^3 - 10x_1^2 - 6x_1 - 1 = 0.$$

Entwickelt man einen Bruch, welcher $f_1(x)$ zum Nenner hat, in eine recurrirende Reihe, muss diese Reihe von Convergenz zu Divergenz übergehen, wenn x_1 durch die gesuchte Wurzel hindurchgeht und dadurch den Bruch unendlich macht; man entwickele deshalb

$$\frac{x^3}{f_1(x)} = 1 + \frac{a_1}{x} + \frac{a_2}{x^2} + \ldots,$$

wo die Coefficienten bestimmt werden durch

$$a_n = 10a_{n-1} + 6a_{n-2} + a_{n-3};$$

dadurch findet man nach und nach

$$1, 10, 106, 1121, 11856, 125392, 1326177 \ldots$$

Zufolge eines Satzes von Cauchy convergirt das Verhältniss zwischen zwei auf einander folgenden Gliedern einer Reihe, welche im Uebergange von Convergenz zu Divergenz begriffen ist, nach 1; dieses Verhältniss ist hier

$$\frac{a_{n+1}}{a_n} \frac{1}{x_1},$$

so dass das Verhältniss

$$\frac{a_n}{a_{a+1}}$$

sich $\frac{1}{x_1}$ nähern muss; durch Benutzuug der beiden letzten berechneten Coefficienten erhält man bereits

$$x = 2 + \frac{1}{x_1} = 2{,}0945514815.$$

Berechnet man noch eihen Coefficienten, so werden dieser und der vorhergehende dieselben 10 Decimalstellen geben.

135. Die hier benutzte Methode stimmt im Wesentlichen mit einer von Daniel Bernoulli angegebenen überein; diese besteht darin, dass man die symmetrischen Functionen der Wurzeln

$$s_m = x_1^{\,m} + x_2^{\,m} + x_3^{\,m} + \cdots$$

$$s_{m+1} = x_1^{\,m+1} + x_2^{\,m+1} + \cdots$$

berechnet; ist nun x_1 die grösste Wurzel, so wird man, für ein hinreichend grosses m, statt s_m und s_{m+1} deren erste Glieder nehmen können, so dass man erhält

$$x_1 = \frac{s_{m+1}}{s_m}.$$

Durch Benutzung von s_{-m} und $s_{-(m+1)}$ kann man auf ähnliche Weise die kleinste Wurzel finden.

Bedenkt man nun, dass

$$\frac{x\,f'(x)}{f(x)} = n + \frac{s_1}{x} + \frac{s_2}{x^2} + \cdots,$$

so sieht man, dass die soeben angewendete Methode mit der von Bernoulli übereinstimmt, sobald man $x\,f'(x)$ zum Zähler nimmt.

Diese Betrachtung zeigt, worauf es ankommt, um die Methode mit Vortheil benutzen zu können; damit alle übrigen Glieder sehr klein im Verhältniss zu $x_1^{\,m}$ werden, darf keine

andere Wurzel nahe bei x_1 belegen sein, ebenso wie die Gleichung keine complexen Wurzeln haben darf, deren Modulus nahe x_1 ist; wendet man die Methode an, um die grösste Wurzel einer Gleichung zu finden, und haben ein Paar complexer Wurzeln einen grösseren Modulus, so wird das Verhältniss zwischen zwei auf einander folgenden Coefficienten sich nicht irgend einem bestimmten Grenzwerthe nähern; sind nämlich die conjugirten complexen Wurzeln

$$r(\cos\theta \pm i\sin\theta),$$

erhält man

$$s_m = 2r^m \cos m\theta + \ldots,$$

$$s_{m+1} = 2r^{m+1}\cos(m+1)\theta + \ldots;$$

aber, selbst wenn die folgenden Glieder vernachlässigt werden können, und also

$$\frac{s_{m+1}}{s_m} = r\frac{\cos(m+1)\theta}{\cos m\theta},$$

erhält man für ein wachsendes m keinen Grenzwerth. Man hat wohl auch in diesem Falle die ganze Reihe benutzen wollen, aber ohne befriedigendes Resultat; die Anwendbarkeit der Methode bleibt deshalb auf den Fall beschränkt, wo es gelingt die Gleichung auf eine solche Form zu bringen, dass die für die Entwicklung benutzten Glieder der Relationsscala dasselbe Zeichen haben und ziemlich stark abnehmen; sie wird deshalb am Besten in Verbindung mit der Methode von Lagrange benutzt, welche im Allgemeinen bald zu einer Gleichung von der angegebenen Form führen wird.

136. Es möge noch ein Beispiel betrachtet werden, nämlich die Gleichung

$$x^3 - 7x + 7 = 0,$$

welche zwei Wurzeln zwischen 1 und 2 hat; setzt man

$$x = 1 + \frac{1}{x_1},$$

so erhält man die Gleichung

$$x_1^3 - 4x_1^2 + 3x_1 + 1 = 0,$$

welche eine Wurzel zwischen 1 und 2 und eine zweite zwischen 2 uud 3 hat; von diesen wird jede einzeln betrachtet; mit Rücksicht auf die letztere setze man

$$x_1 = 2 + \frac{1}{x_2},$$

woraus die Gleichung

$$x_2^3 + x_2^2 - 2x_2 - 1 = 0,$$

deren positive Wurzel zwischen 1 und 2 liegt; also setze man

$$x_2 = 1 + \frac{1}{x_3},$$

wodurch

$$x_3^3 - 3x_3^2 - 4x_3 - 1 = 0;$$

die positive Wurzel dieser Gleichung liegt zwischen 4 und 5; endlich setze man

$$x_3 = 4 + \frac{1}{x_4},$$

wodurch die transformirte Gleichung

$$x_4^3 - 20x_4^2 - 9x_4 - 1 = 0$$

wird; hier ist die Relationsscala

20, 9, 1,

und mit Hülfe dieser berechnet man die Coefficienten

1, 20, 409, 8361, 170921, 3494078, . . .

Setzt man nun

$$x_4 = \frac{3494078}{170921},$$

so hat man

$$x = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{x_4}}}}$$

oder

$$x = \frac{19 . 3494078 + 4 . 170921}{14 . 3494078 + 3 . 170921} = 1{,}3568958\ldots,$$

wo alle angeführten Decimalstellen richtig sind.

137. Neben der Methode von Bernoulli ist noch die von Gräffe zu erwähnen. Diese besteht darin, dass man $x = \sqrt{y}$ setzt und die Wurzelzeichen fortschafft, wodurch eine Gleichung gebildet wird, deren Wurzeln die Quadrate der Wurzeln der gegebenen sind; man fährt nun auf dieselbe Weise fort, indem man mit den Logarithmen der Coefficienten rechnet; wenn eine neue Transformation die Logarithmen der Coefficienten doppelt so gross macht, so ist das ein Zeichen dafür, dass die kleineren Wurzeln im Verhältniss zu den grösseren als verschwindend betrachtet werden können; es werde z. B. angenommen, dass die Wurzeln auf die 32ste Potenz erhoben worden wären und dadurch die Gleichung

$$z^n + a_1 z^{n-1} + a_2 z^{n-2} + \ldots = 0$$

erhalten sei; dann setzt man

$$x_1^{32} = -a_1$$
$$x_1^{32} x_2^{32} = a_2$$
$$x_1^{32} x_2^{32} x_3^{32} = -a_3 \text{ u. s. w.},$$

indem man überall nur das höchste Glied behält; man findet dadurch alle Wurzeln, falls dieselben reell sind, aber man hat dieselben Schwierigkeiten mit den complexen Wurzeln wie bei Bernoulli's Methode, welche auf dieselbe Idee gegründet ist. Das Detail der Methode kann deshalb übergangen werden.

Methode von Horner.

138. Horner's Methode stützt sich im Wesentlichen darauf, dass man aus einer gegebenen Gleichung eine andere bilden

kann, deren Wurzeln um eine gewisse Grösse kleiner sind als die Wurzeln der gegebenen Gleichung. Die Methode erhält indessen namentlich ihre Bedeutung dadurch, dass sie ein gleichmässiges und einfaches Verfahren zur Ausführung dieser Transformation angiebt.

Die gegebene Gleichung sei

$$f(x) = 0;$$

die Gleichung, deren Wurzeln um α kleiner sind, erhält man dann dadurch, dass man die gegebene Gleichung so umformt, dass $x - \alpha$ die neue Unbekannte wird; zu dem Zwecke setzt man

$$f(x) = f(\alpha + x - \alpha) = f(\alpha) + f'(\alpha)(x - \alpha) + \frac{f''(\alpha)}{1.2}(x - \alpha)^2 \ldots + (x - \alpha)^n = 0.$$

Hieraus ist ersichtlich, dass $f(\alpha)$ der Rest ist, welchen man erhält, wenn man $f(x)$ durch $x - \alpha$ dividirt, $f'(\alpha)$ der Rest, welchen man bekommt, wenn man den erhaltenen Quotienten wiederum durch $x - \alpha$ dividirt u. s. w.; durch wiederholte Division mit $x - \alpha$ erhält man also alle Coefficienten der transformirten Gleichung.

Zur Ausführung der Division mit $x - \alpha$ bedient man sich der Methode, durch welche ein Bruch in eine Reihe entwickelt wird; die Relationsscala ist α; ist nun der Dividendus

$$a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n$$

und der Quotient

$$b_0 x^{n-1} + b_1 x^{n-2} + b_2 x^{n-3} \ldots + b_{n-1} + \frac{b_n}{x - \alpha},$$

so hat man

$$b_0 = a_0;\ b_1 = a_1 + \alpha b_0;\ b_2 = a_2 + \alpha b_1;\ \ldots b_p = a_p + \alpha b_{p-1} \ldots$$

Man pflegt der Rechnung eine bestimmte Form zu geben; um diese zu zeigen, mögen die Wurzeln der Gleichung

$$3x^5 - x^3 + 4x^2 + 5x - 8 = 0$$

um 2 kleiner gemacht werden; man erhält dann, wenn man nur die Coefficienten schreibt,

$$\begin{array}{rrrrrr}
3 & 0 & -1 & +4 & +5 & -8 \\
3 & 6 & 11 & 26 & 57 & 106 \\
3 & 12 & 35 & 96 & 249 & \\
3 & 18 & 71 & 238 & & \\
3 & 24 & 119 & & & \\
3 & 30 & & & &
\end{array}$$

und die transformirte Gleichung wird also

$$3x^5 + 30x^4 + 119x^3 + 238x^2 + 249x + 106 = 0.$$

Die Multiplication mit 2 (α) und die Addition ist hier gleichzeitig ausgeführt worden; sind die Zahlen grösser, so dass diese Rechnung nicht mit Sicherheit im Kopfe gemacht werden kann, so thut man am besten das Product $\alpha\, b_p$ unter a_{p+1} zu schreiben und darauf zu addiren, wie es bei dem Beispiel weiter unten geschehen ist.

Man bedient sich nun dieser Methode um nach und nach die Ziffern der Wurzel, eine aufs Mal, zu finden; liegt die Wurzel z. B. zwischen 2 und 3, so werden die Wurzeln um 2 kleiner gemacht; für die transformirte Gleichung wird nun die erste Decimalstelle der Wurzel gesucht, wozu man nur die beiden letzten Glieder benutzt; findet man nun, dass diese z. B. 5 ist, wird die Wurzel um 0,5 kleiner gemacht, und nun kann man auf diese Weise fortfahren. Es kann sich ereignen, dass man einen zu grossen Werth für die gesuchte Decimale erhält; das wird sich dadurch zu erkennen geben, dass das letzte Glied der Gleichung bei der Transformation das Zeichen wechselt, weil eine der Wurzeln das Zeichen gewechselt hat; man muss dann zurückgehen und die nächst niedrigere Ziffer versuchen; ist die durch die beiden letzten Glieder bestimmte Ziffer zu klein, so wird das bald bemerkt werden, wenn man weiter rechnet.

Als Beispiel möge die früher untersuchte Gleichung

$$x^3 - 7x + 7 = 0$$

dienen; es soll die Wurzel gesucht werden, welche zwischen

1,3 und 1,4 liegt; die Rechnung sieht dann folgendermassen aus:

1	0	-7	$+7$
1	1	-6	$+1$
1	2	-4	
1	3		
1	0,3	0,99	$-0,903$
1	3,3	$-3,01$	0,097
1	0,3	1,08	
1	3,6	$-1,93$	
1	0,3		
1	3,9		

Die Wurzel ist nun um 1,3 kleiner gemacht worden; die nächste Ziffer wird bestimmt durch

$$1,93\,x = 0,097; \quad x = 0,05;$$

man macht deshalb jetzt die Wurzel um 0,05 kleiner:

1	3,9	$-1,93$	0,097
1	0,05	0,1975	$-0,086625$
	3,95	$-1,7325$	0,010375
	0,05	0,20	
	4,00	$-1,5325$	
	0,05		
	4,05		

Die beiden letzten Glieder geben nun die Ziffer 6; also

1	4,05	$-1,5325$	0,010375
	0,006	0,024336	$-0,009048984$
	4,056	$-1,508164$	0,001326016
	0,006	0,024372	
	4,062	$-1,483792$	
	0,006		
	4,068		

Hiernach wird die nächste Ziffer 8 sein.

139. Nachdem man auf solche Weise einige Ziffern gefunden hat, kann man die folgenden durch eine abgekürzte Rechnung finden; man sieht nämlich, dass man, um die Ziffer 8 zu finden, nicht die vier letzten Decimalstellen der

beiden letzten Reihen nöthig hat; für jede neue Ziffer, welche man sucht, streicht man deshalb die beiden letzten Decimalstellen der ersten Reihe (hier von 4,068) und die entsprechende Anzahl in den übrigen Reihen; bei der Multiplication berücksichtigt man die gestrichenen Ziffern, so dass man hier z. B. hat

$$8 . 40(68) = 325;$$

auf die Weise erhält man, wenn man die Nullen fortlässt:

1	4,0(68)	— 1,483792	0,001326016 (8956)
		325	— 1184432
		— 1,48054	0,000141584
		4	— 133209
		— 1,4801	8375
		— 1,480	7401
		— 1,48	974
			888
			86

Man erhält also auf diese Weise

$$x = 1,3568957,$$

wo die letzte Decimale erhöht worden ist; nach dem vorhergehenden würde die letzte Decimale 8 sein.

Berechnung der complexen Wurzeln.

140. In 110 wurde gezeigt, dass die Absonderung der complexen Wurzeln erfolgen kann, indem man die Grenzen für den Modulus und das Argument der Wurzel sucht, oder indem man die Grenzen bestimmt, zwischen welchen der reelle und zwischen welchen der imaginäre Theil der Wurzel belegen ist; darauf kann man Newton's Methode benutzen um die Wurzel genauer zu bestimmen; im Allgemeinen wird die Rechnung aber sehr beschwerlich werden, da man nicht ohne genauere Untersuchung entscheiden kann, ob Newton's

Formel in Wirklichkeit näher an die gesuchte Wurzel heranführt. Man pflegt deshalb ein anderes Verfahren einzuschlagen, wodurch die Aufgabe darauf zurückgeführt wird, die reellen Wurzeln einer Hülfsgleichung zu bestimmen.

Die Gleichung sei

$$f(x) = 0$$

und man setze

$$x = y + iz.$$

Dann erhält man

$$f(y) + f'(y)\,iz - f''(y)\frac{z^2}{1.2} - f'''(y)\frac{z^3 i}{1.2.3}\ldots = 0,$$

welche Gleichung in die beiden anderen

$$f(y) - f''(y)\frac{z^2}{1.2} + f^{IV}(y)\frac{z^4}{1.2.3.4} - \ldots = 0$$

und

$$f'(y) - f'''(y)\frac{z^2}{1.2.3} + f^{V}(y)\frac{z^4}{5!} - \ldots = 0$$

zerfällt.

Wird y aus diesen beiden Gleichungen eliminirt, so erhält man eine Gleichung in z, welche, da sie nur z mit geraden Exponenten enthält, auf den halben Grad reducirt werden kann. Durch eine der oben angegebenen Methoden bestimmt man nun die positiven Werthe von z^2; ausserdem ist bekannt, dass die Elimination zu einer Gleichung führt, durch welche man y rational durch z^2 ausgedrückt erhält, und welche also für jeden Werth von z^2 den zugehörigen Werth von y giebt. Es wurde vorausgesetzt, dass die gegebene Gleichung reelle Coefficienten habe, und dass nur ein Paar conjugirter Wurzeln denselben imaginären Theil habe, so dass jedem Werthe von z^2 nur ein Werth von y entspricht; sind zwei Paare conjugirter Wurzeln vorhanden, welche den gleichen imaginären Theil haben, wird y, nachdem z^2 gefunden ist, durch

eine Gleichung zweiten Grades bestimmt werden u. s. w., wie es bei der Eliminationstheorie gezeigt worden ist.

Man wird die Bedeutung dieser Methode besser verstehen, wenn man sie von einer anderen Seite betrachtet; bezeichnet man ein Paar conjugirter Wurzeln mit x_1 und x_2, hat man

$$x_1 = y_1 + i z_1, \; x_2 = y_1 - i z_1,$$

also

$$y_1 = \frac{1}{2}(x_1 + x_2),$$

$$z_1^2 = -\frac{1}{4}(x_1 - x_2)^2.$$

Die Gleichung in z^2 wird also, nach einer geringen Veränderung, mit der Gleichung der quadrirten Wurzeldifferenzen übereinstimmen; diese erhält eine negative Wurzel für jedes Paar conjugirter Wurzeln der gegebenen Gleichung, eine positive Wurzel für jede Combination von zwei reellen Wurzeln, und eine complexe Wurzel für jede Combination von einer reellen und einer complexen oder von zwei complexen nicht conjugirten Wurzeln der gegebenen Gleichung.

Beisp.

$$x^4 + a x^2 + b x + c = 0.$$

Man erhält

$$y^4 + a y^2 + b y + c - (6 y^2 + a) z^2 + z^4 = 0,$$
$$4 y^3 + 2 a y + b - 4 y z^2 = 0,$$

woraus, durch Elimination von z^2,

$$y^6 + \frac{a}{2} y^4 + \frac{a^2 - 4c}{16} y^2 - \frac{b^3}{64} = 0,$$

$$z^2 = y^2 + \frac{a}{2} + \frac{b}{4y}.$$

Für

$$x^4 - x + 1 =$$

werden die beiden Gleichungen

$$y^6 - \frac{1}{4}y^2 - \frac{1}{64} = 0;\ z^2 = y^2 - \frac{1}{4y}.$$

Setzt man $y^2 = \frac{v}{4}$, so erhält man

$$v^3 - 4v - 1 = 0,$$

oder, wenn die Wurzeln um 2 kleiner gemacht werden,

$$v_1^3 + 6v_1^2 + 8v_1 - 1 = 0.$$

Nun kann man die Entwicklung in eine recurrirende Reihe benutzen. Die Relationsscala ist

$$8 \quad 6 \quad 1,$$

wodurch man erhält

$$1 \quad 8 \quad 70 \quad 609 \quad 5300 \quad 46124\ldots,$$

$$v = 2 + \frac{5300}{46124} = 2{,}1149076\ldots,$$

$$y^2 = 0{,}5287269\ldots,\ y = \pm 0{,}727136\ldots,$$

$$z^2 = \begin{cases} 0{,}8725415\ldots \\ 0{,}1849123\ldots \end{cases}$$

und daraus die vier Wurzeln

$$-0{,}727136\ldots \quad \pm i\,.\,0{,}934092\ldots$$

$$+0{,}727136\ldots \quad \pm i\,.\,0{,}430014\ldots$$

VIERTER ABSCHNITT.

UEBER SUBSTITUTIONEN.

Erstes Kapitel.

Ueber Substitutionen im Allgemeinen.

Ordnung der Substitutionen.

141. Aus einer Function von n Grössen kann man eine andere durch Vertauschung dieser Grössen bilden; so wird

$$x_1 + 2x_2 + 3x_3$$

aus

$$x_2 + 2x_3 + 3x_1$$

gebildet, wenn man x_1 an die Stelle von x_2, x_2 an die von x_3 und x_3 an die von x_1 setzt. Die Operation, welche man ausführt, indem man auf solche Weise gewisse Buchstaben durch andere ersetzt, heisst eine *Substitution;* man bezeichnet dieselbe durch zwei Reihen Buchstaben, die so zu verstehen sind, dass jeder Buchstabe der unteren Reihe, wo er in der Function vorkommt, durch den Buchstaben ersetzt werden soll, welcher gerade darüber in der anderen Reihe steht. Die oben ausgeführte Substitution wird also

$$\begin{pmatrix} x_3 & x_1 & x_2 \\ x_1 & x_2 & x_3 \end{pmatrix}$$

geschrieben. Da es nur darauf ankommt, welche Buchstaben

über einander stehen, kann man die Buchstaben der unteren Reihe in beliebiger Reihenfolge schreiben.

Die allgemeine Bezeichnung für eine Substitution wird deshalb

$$S = \binom{A_1}{A_0},$$

wo A_1 und A_0 zwei Permutationen der n Buchstaben bedeuten. A_0 heisst der Nenner, A_1 der Zähler; der Buchstabe, welcher bei der Substitution an die Stelle eines anderen kommt, soll der *Ablöser* desselben heissen.

Lässt man A_0 unverändert, so können an Stelle von A_1 $n!$ verschiedene Permutationen gesetzt werden, und diese Zahl bestimmt deshalb die Anzahl der für n Buchstaben möglichen Substitutionen; von diesen wird die eine

$$\binom{A_0}{A_0},$$

welche angiebt, dass alle Buchstaben an ihrer Stelle bleiben, und welche durch die Zahl 1 bezeichnet wird.

Stehen in einer Substitution zwei gleiche Buchstaben über einander, so können dieselben ausgelassen werden; die Substitution versetzt dann die Buchstaben, welche in ihr vorkommen, und keine anderen.

Schreibt man

$$S A_0,$$

so bedeutet das, dass die Substitution S auf die Permutation A_0 angewendet werden soll; man hat dann

$$\binom{A_1}{A_0} A_0 = A_1.$$

Das Product von zwei Substitutionen

$$T S$$

bezeichnet die Substitution, welche man ausführt, indem man

erst die Substitution S und darauf im Resultate die Substitution T ausführt; man hat dann z. B.

$$\begin{pmatrix} A_2 \\ A_1 \end{pmatrix} \begin{pmatrix} A_1 \\ A_0 \end{pmatrix} = \begin{pmatrix} A_2 \\ A_0 \end{pmatrix}.$$

Im Allgemeinen ist die Reihenfolge der Factoren hier nicht gleichgültig.

Dass die Substitution S p Male ausgeführt werden soll, wird durch

$$S^p$$

bezeichnet; man hat deshalb

$$S^0 = 1,$$

indem man durch beide Ausdrücke bezeichnet, dass keine Vertauschung von Buchstaben stattfinden soll.

Falls

$$S = T,$$

so ist auch, wie leicht ersichtlich

$$S S_1 = T S_1 \text{ und } S_1 S = S_1 T,$$

so dass man beide Seiten einer Gleichung mit derselben Substitution multipliciren kann, indem man beiderseits den Factor rechts oder beiderseits links stellt.

Beisp. Aus

$$x_1 x_2^2 + x_3^3 x_4$$

wird durch die Substitution

$$S = \begin{pmatrix} x_4 & x_1 & x_2 & x_3 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}$$

$$x_4 x_1^2 + x_2^3 x_3$$

gebildet.

Ist

$$T = \begin{pmatrix} x_3 & x_1 & x_2 \\ x_1 & x_2 & x_3 \end{pmatrix},$$

so wird

$$S\,T = \begin{pmatrix} x_2 & x_4 & x_1 & x_3 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}; \quad T\,S = \begin{pmatrix} x_4 & x_3 & x_1 & x_2 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}$$

$$S^2 = \begin{pmatrix} x_3 & x_4 & x_1 & x_2 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}; \quad T^2 = \begin{pmatrix} x_2 & x_3 & x_1 \\ x_1 & x_2 & x_3 \end{pmatrix} \text{ u. s. w.}$$

142. Wenn man aus der Substitution S eine Reihe von Substitutionen

$$1, S, S^2 \ldots$$

bildet, muss man, da die ganze mögliche Anzahl von Substitutionen endlich ist, einmal zu einer Substitution kommen, welche man schon früher gehabt hat; beispielsweise werde angenommen, dass

$$S^{\alpha+\beta} = S^{\alpha}$$

oder

$$S^{\beta} S^{\alpha} = S^{\alpha};$$

diese Gleichung zeigt, dass jede Permutation durch die Substitution S^{β} unverändert bleibt, so dass man

$$S^{\beta} = 1$$

hat, woraus wiederum, wenn k eine beliebige ganze Zahl ist, folgt

$$S^{k\beta+\alpha} = S^{\alpha};$$

daraus geht hervor, dass die Potenzen von S eine periodische Reihe bilden.

Ist β der kleinste Werth, für welchen $S^{\beta} = 1$, so sagt man, die Substitution sei von der Ordnung β.

Anstatt $S^{\beta-\alpha}$ schreibt man auch $S^{-\alpha}$; man hat dann

$$S^{-\alpha} S^{\alpha} = 1.$$

Man sieht leicht, dass, wenn a b in S ablöst, b a in S^{-1} ablösen wird.

S sei von der Ordnung β und

$$\beta = f\beta_1, \; \alpha = f\alpha_1,$$

wo f der grösste gemeinschaftliche Factor von β und α ist, so dass β_1 und α_1 relative Primzahlen sind. Um die Ordnung x der Substitution S^α zu bestimmen setze man dann

$$(S^\alpha)^x = 1 = S^{k\beta},$$

woraus

$$x = \frac{k\beta}{\alpha} = \frac{k\beta_1}{\alpha_1};$$

hieraus geht hervor, dass β_1 oder $\frac{\beta}{f}$ der kleinste Werth für die ganze Zahl x ist; also:

Wenn S von der Ordnung β ist, wird S^α von der Ordnung $\frac{\beta}{f}$ sein, wo f der grösste gemeinschaftliche Factor von α und β ist; im Besonderen ist zu beachten, *dass die beiden Substitutionen von derselben Ordnung sind, sobald α und β prim zu einander sind.* In diesem letzten Falle werden die Potenzen von S^α dieselben Substitutionen wie die Potenzen von S, nur in einer anderen Reihenfolge, geben; setzt man nämlich

$$(S^\alpha)^x = S^p = S^{y\beta + p},$$

so wird x durch die unbestimmte Gleichung

$$\alpha x - \beta y = p$$

bestimmt, welche, wie bekannt, immer eine Lösung hat, sobald α und β prim zu einander sind.

Beisp. Aus

$$S = \begin{pmatrix} e & a & c & b & d \\ a & b & c & d & e \end{pmatrix} = \begin{pmatrix} e & a & b & d \\ a & b & d & e \end{pmatrix}$$

erhält man

$$S^2 = \begin{pmatrix} d & e & a & b \\ a & b & d & e \end{pmatrix},$$

$$S^3 = \begin{pmatrix} b & d & e & a \\ a & b & d & e \end{pmatrix},$$

$$S^4 = \begin{pmatrix} a & b & d & e \\ a & b & d & e \end{pmatrix} = 1,$$

so dass diese Substitution von der vierten Ordnung ist; setzt man z. B.

$$(S^3)^x = S^2 = S^{4y+2},$$

so erhält man

$$3x - 4y = 2;\ x = 2;$$

man hat auch

$$(S^3)^2 = \begin{pmatrix} d & e & a & b \\ a & b & d & e \end{pmatrix} = S^2.$$

Wird diese letzte Substitution auf die Function

$$a^3 + 3ab^2 - 2cde$$

angewendet, so erhält man

$$d^3 + 3de^2 - 2cab.$$

Cyclische Substitutionen.

143. Eine Substitution heisst *cyclisch*, wenn die darin vorkommenden Buchstaben in einer solchen Reihe aufgestellt werden können, dass jeder von ihnen durch die Substitution von dem nächsten, der letzte von dem ersten abgelöst wird; so ist in dem obigen Beispiel S cyclisch, wenn man c von der Betrachtung ausschliesst; denn nimmt man die Reihe

$$a\ e\ d\ b,$$

so wird eben jeder Buchstabe durch den folgenden ersetzt; eine solche Substitution wird auch durch eine Reihe von Buchstaben in Klammern bezeichnet; auf die Weise hat man

$$S = \begin{pmatrix} b\,c\,d\,e\,a \\ a\,b\,c\,d\,e \end{pmatrix} = (a\,b\,c\,d\,e) = (b\,c\,d\,e\,a) \text{ u. s. w.}$$

Die Ordnung einer cyclischen Substitution ist offenbar gleich der Anzahl der Buchstaben, welche versetzt werden, denn bei jedesmaliger Ausführung der Substitution wird ein Buchstabe des Zählers um einen Platz nach links gerückt; über a werden deshalb nach und nach b, c, d, e, a zu stehen kommen, und wenn a über a steht, hat man die Substitution 1.

144. *Jede Substitution kann als ein Product von cyclischen Substitutionen dargestellt werden.*

Man nehme nämlich einen beliebigen Buchstaben des Nenners; nimmt man nun dessen Ablöser, darauf wieder dessen Ablöser und so fort, bis man wieder den ersten Buchstaben trifft, so bilden alle diese eine cyclische Substitution oder einen *Cyclus* der gegebenen Substitution; die übriggebliebenen Buchstaben werden dann auf dieselbe Weise behandelt. Eine Substitution von zwei Buchstaben heisst eine *Transposition;* sie bedeutet, dass zwei Buchstaben vertauscht werden sollen; ein Cyclus von einem Buchstaben kann ausgelassen werden.

Aus

$$S = \begin{pmatrix} h & k & d & f & b & j & a & g & e & c & i & m & l & n \\ a & b & c & d & e & f & g & h & i & j & k & l & m & n \end{pmatrix}$$

erhält man demgemäss

$$S = (a\,h\,g)\,(b\,k\,i\,e)\,(c\,d\,f\,j)\,(l\,m)\,(n),$$

wo der letzte Cyclus von einem Buchstaben fortgelassen werden kann. Es leuchtet ein, dass die Reihenfolge von solchen Cyclen und im Allgemeinen von Factoren, welche lauter verschiedene Buchstaben enthalten, gleichgültig ist.

145. *Die Ordnung einer Substitution ist gleich dem kleinsten gemeinschaftlichen Vielfachen der Zahlen, welche die Ordnung der Cyclen der Substitution angeben.*

Ist nämlich

$$S = C_0\, C_1\, C_2 \ldots$$

die in Cyclen zerlegte Substitution, und soll man

$$S^x = 1$$

haben, so muss dies, da die Cyclen verschiedene Buchstaben enthalten, mit sich führen, dass

$$C_0{}^x = 1,\ C_1{}^x = 1,\ C_2{}^x = 1 \ldots;$$

der kleinste Werth von x ist deshalb die kleinste Zahl, in welcher die Zahlen, welche die Ordnung der Cyclen angeben, aufgehen.

Sind alle Cyclen von derselben Ordnung, so ist diese auch die Ordnung von S, und eine solche Substitution heisst *regelmässig;* dabei ist indessen wohl zu beachten, dass nach der Voraussetzung derselbe Buchstabe nicht in zwei Cyclen vorkommen darf. (a b) (c d) ist regelmässig und von zweiter Ordnung, aber (a b) (b c) = (a b c) ist cyclisch von dritter Ordnung.

146. *Falls S cyclisch von der Ordnung* β *ist, wird* S^α *regelmässig sein und aus f Cyclen bestehen, wenn f der grösste gemeinschaftliche Factor von* β *und* α *ist*; sind α und β prim zu einander, so wird S^α selber cyclisch.

Ist nämlich

$$S = (a_1\, a_2 \ldots a_\beta),$$

so wird hierin a_p von a_{p+1} abgelöst werden; in S^2 wird a_p von a_{p+2} und in S^α von $a_{p+\alpha}$ abgelöst werden; man kann also den Cyclus

$$(a_p\, a_{p+\alpha}\, a_{p+2\alpha} \cdots)$$

bilden, wo ein grösserer Index als β den Rest bezeichnet, den derselbe bei der Division mit β giebt. Um zu a_p zu gelangen, muss man deshalb

$$p + x\alpha = p + y\beta \text{ oder } x = \frac{y\beta}{\alpha}$$

haben, wo x die Anzahl der Buchstaben des Cyclus darstellt; sind nun α und β prim zu einander, muss $y = \alpha$, $x = \beta$ sein, so dass die erhaltene Substitution cyclisch ist; ist $\alpha = f\alpha_1$, $\beta = f\beta_1$, muss $y = \frac{\alpha}{f}$ sein, also die Anzahl der Cyclen

$$\frac{\beta}{x} = f.$$

Beisp.

$$\begin{aligned} S &= (a\,b\,c\,d\,e\,f), \\ S^2 &= (a\,c\,e)\,(b\,d\,f), \\ S^3 &= (a\,d)\,(b\,e)\,(c\,f), \\ S^4 &= (a\,e\,c)\,(b\,f\,d), \\ S^5 &= (a\,f\,e\,d\,c\,b), \\ S^6 &= 1. \end{aligned}$$

147. *Jede regelmässige Substitution ist eine Potenz einer cyclischen Substitution.*

Ist nämlich die regelmässige Substitution

$$S = (a_1\,b_1\,c_1 \dots g_1)\,(a_2\,b_2\,c_2 \dots g_2) \dots (a_m\,b_m\,c_m \dots g_m),$$

und setzt man

$$C = (a_1\,a_2 \dots a_m\,b_1\,b_2 \dots b_m \dots g_1\,g_2 \dots g_m)$$

so ist offenbar

$$S = C^m.$$

148. *Jede Substitution kann in primitive Factoren zerlegt werden,* das heisst in solche Factoren, deren Ordnung eine Primzahl oder eine Potenz einer Primzahl ist.

Wenn S von der Ordnung n ist und

$$n = \alpha\beta,$$

wo α und β prim zu einander sind, kann man nämlich immer zwei ganze Zahlen x und y von der Beschaffenheit finden, dass

$$\alpha x + \beta y = 1,$$

also

$$S = S^{\alpha x} S^{\beta y}.$$

Hier ist

$$(S^{\alpha x})^{\beta} = 1; \ (S^{\beta y})^{\alpha} = 1,$$

so dass von den beiden Factoren der eine von der Ordnung β, der andere von der Ordnung α ist. Diese Zerlegung kann nun so lange fortgesetzt werden, als die Ordnung in Factoren zerlegt werden kann, die prim zu einander sind, also bis die Ordnung jedes Factors eine Primzahl oder eine Potenz von einer Primzahl ist.

Beisp.

$$S = (a\,b\,c\,d\,e\,f)$$

ist von der Ordnung 2 . 3; dadurch erhält man

$$S = S^3 S^4,$$

wo

$$S^3 = (a\,d)\,(b\,e)\,(c\,f),$$

$$S^4 = (a\,e\,c)\,(b\,f\,d).$$

Ueber ähnliche und vertauschbare Substitutionen.

149. Zwei Substitutionen heissen *ähnlich*, wenn sie aus gleich vielen Cyclen bestehen, und diese beziehungsweise gleich viele Buchstaben enthalten; zwei Substitutionen S und T heissen *vertauschbar*, wenn

$$S\,T = T\,S.$$

Die Substitution

$$A S A^{-1}$$

heisst *die Transformirte von S durch A.*

150. *Eine Substitution ist ihrer Transformirten ähnlich.*

Sei

$$(a\, b\, c \ldots)$$

einer der Cyclen von S, und a_1, b_1, $c_1 \ldots$ seien die Buchstaben, welche a, b, c... in A ablösen. Bei Anwendung von A^{-1} wird dann a_1 von a abgelöst werden, welches durch S wiederum von b abgelöst wird, und dieses wird wiederum durch A von b_1 abgelöst. In der Transformirten

$$A S A^{-1}$$

wird also a_1 von b_1 abgelöst werden, also auch b_1 von $c_1 \ldots$, so dass einer der Cyclen

$$(a_1\, b_1\, c_1 \ldots)$$

wird.

Die Transformirte durch A wird also aus S gebildet, indem man in den Cyclen von S die Buchstaben durch ihre Ablöser in A ersetzt.

Beisp.

$$S = (a\, b\, c\, d);\; A = (a\, c)\, (b\, d);\; A S A^{-1} = (c\, d\, a\, b).$$

Ist

$$S = (a\, b\, c)\, (d\, e),$$

$$T = (d\, c\, a)\, (b\, e),$$

wird

$$T = A S A^{-1},$$

wo

$$A = (a\, d\, b\, c).$$

Also: *Wenn S und T ähnlich sind, kann man immer eine Substitution A finden, durch welche S in T transformirt*

wird; diese Substitution bildet man nämlich dadurch, dass man jeden Buchstaben in T zu dem Ablöser desjenigen macht, welcher auf dem entsprechenden Platze in S steht.

151. *Die beiden Producte, welche aus zwei beliebigen Substitutionen gebildet werden können, sind ähnlich.*

S T und T S sind ähnlich, weil

$$S\,T = S\,(T\,S)\,S^{-1}.$$

152. *Die Transformirte eines Productes ist gleich dem Producte der Transformirten der Factoren.*

$$A\,(S\,T)\,A^{-1} = A\,S\,A^{-1}\,A\,T\,A^{-1}.$$

153. *Wenn zwei Substitutionen vertauscht werden können, können ihre Transformirten auch vertauscht werden,* denn aus

$$S\,T = T\,S$$

folgt

$$A\,S\,A^{-1}\,A\,T\,A^{-1} = A\,T\,A^{-1}\,A\,S\,A^{-1}.$$

154. Wenn die Substitutionen S und T vertauscht werden können, hat man

$$S\,T = T\,S \text{ oder } S = T\,S\,T^{-1},$$

so dass S unverändert bleiben muss, wenn sie durch T transformirt wird. Da man diese Transformation ausführt, indem man T auf die Cyclen von S anwendet (150), so müssen diese durch die Transformation entweder unverändert bleiben oder unter einander vertauscht werden. Der erste Fall tritt ein, wenn die Buchstaben des Cyclus nicht in T vorkommen, oder wenn eine Potenz des Cyclus ein Factor von T ist, so dass der Cyclus nur mit einem anderen Buchstaben als vorher beginnt, aber ohne dass die Reihenfolge der Buchstaben verändert wird. Ausser derartigen Factoren kann T deshalb nur solche enthalten, durch welche die Cyclen vertauscht werden; ein solcher Factor von T soll nun genauer untersucht werden.

Wird dieser Factor auf den Cyclus C_1 angewendet, so geht dieser in einen anderen C_2 über, der auch in S vorkommen muss; C_2 geht in C_3 über, der auch in S vorkommen muss, und so fort, bis ein gewisser Cyclus C_μ in C_1 übergeht; doch kann es sich hierbei ereignen, dass C_1 mit einem anderen Buchstaben beginnt, als ursprünglich der Fall war, während die übrigen Cyclen so geschrieben werden können, wie jeder derselben durch Transformation aus dem vorhergehenden hervorgeht; man hat also z. B.

$$C_1 = (a_1\, a_2 \dots a_i)$$
$$C_2 = (b_1\, b_2 \dots b_i)$$
$$\dots\dots\dots\dots$$
$$\dots\dots\dots\dots$$
$$C_\mu = (f_1\, f_2 \dots f_i),$$

wo C_μ übergeht in

$$(a_{\rho+1}\, a_{\rho+2} \dots a_\rho).$$

Der Factor von S

$$P = C_1\, C_2 \dots C_\mu$$

ist eine regelmässige Substitution; ist $\rho = 0$, so ist der Factor Q von T auch regelmässig, nämlich

$$Q = (a_1\, b_1 \dots f_1)\,(a_2\, b_2 \dots f_2)\,(a_i\, b_i \dots f_i).$$

Für andere Werthe von ρ wird Q auch regelmässig, aber die Anzahl der Buchstaben in jedem Cyclus wird ein Vielfaches von μ; der erste Cyclus wird nämlich, wenn man die Indices nach dem Modulus i nimmt,

$$(a_1\, b_1\, c_1 \dots f_1\, a_{\rho+1}\, b_{\rho+1} \dots f_{\rho+1}\, a_{2\rho+1} \dots),$$

wo man zuletzt zu einem Gliede

$$a_{q\rho+1}$$

gelangen muss, welches das Glied a_1 ist; also muss

$$q\rho = ki$$

sein, oder, wenn α der grösste gemeinschaftliche Factor für ρ und i ist, und $\alpha\rho_1 = \rho$; $\alpha i_1 = i$,

$$q\rho_1 = k i_1,$$

mithin

$$q = i_1;$$

Q ist also cyclisch mit $i_1 \mu$ Buchstaben in jedem Cyclus und α Cyclen.

Man hat nun

$$P^\rho = (a_1\, a_{1+\rho}\, a_{1+2\rho} \ldots)(b_1\, b_{1+\rho} \ldots) \ldots,$$

$$Q^\mu = (a_1\, a_{1+\rho}\, a_{1+2\rho} \ldots)(b_1\, b_{1+\rho} \ldots) \ldots,$$

also

$$P^\rho = Q^\mu,$$

und diese Potenzen müssen von 1 verschieden sein, da P von der Ordnung i ist und $\rho < i$. S und T können also nur vertauscht werden, wenn ihre gemeinschaftlichen Buchstaben regelmässige Substitutionen bilden, welche einander paarweise auf die hier bestimmte Weise entsprechen. Die Gleichung $P^\rho = Q^\mu$ drückt eine nothwendige aber keine ausreichende Bedingung dafür aus, dass P und Q gegen einander vertauscht werden können.

155. *Man kann immer solche Substitutionen T finden, dass*

$$S^m = T\,S\,T^{-1}, \ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

wenn m prim zu der Ordnung von S ist.

m muss nämlich prim zu der Ordnung jedes der Cyclen von S sein. S^m ist dann S ähnlich, weil jeder der Cyclen durch Potenziren einen neuen Cyclus mit denselben Buchstaben giebt. Es giebt dann Werthe von T (150); einer von diesen sei T_1. (1) kann dann auf die Form

$$T_1\,S\,T_1^{-1} = T\,S\,T^{-1}$$

oder

$$S T_1^{-1} T = T_1^{-1} T S$$

gebracht werden, woraus hervorgeht, dass S und $T_1^{-1} T$ vertauscht werden können; nun möge U eine beliebige Substitution sein, welche gegen S vertauscht werden kann, und es sei

$$T_1^{-1} T = U,$$

woraus

$$T = T_1 U.$$

Diese Substitution befriedigt (1), denn man hat

$$T_1 U S (T_1 U)^{-1} = T_1 S T_1^{-1} = S^m;$$

man sieht hieraus, *dass man alle Lösungen von (1) erhält, wenn man alle Substitutionen, welche gegen S vertauscht werden können, mit einer der Lösungen multiplicirt.*

Beisp.

$$S = (a\,b\,c)\,(d\,e\,f); \; S^2 = (a\,c\,b)\,(d\,f\,e);$$

$$S^2 = T S T^{-1}, \text{ wenn } T = (b\,c)\,(e\,f).$$

Positive und negative Substitutionen.

156. *Eine beliebige Substitution kann in ein Product von Transpositionen zerlegt werden.*

Man kann nämlich einen der Buchstaben durch eine Transposition auf den Platz bringen, welchen derselbe einnehmen soll; es bleibt dann übrig eine Substitution auszuführen, in welcher dieser Buchstabe fehlt, und welche wiederum auf dieselbe Weise behandelt werden kann. Auf die Weise hat man z. B.

$$(a\,b\,c\,d) = (b\,d)\,(b\,c)\,(a\,d).$$

156. *Nur eine gerade Anzahl von Transpositionen kann zum Producte 1 haben.*

Es seien a, b, c, d ... die Buchstaben, welche vertauscht werden sollen, und man betrachte das Product

$$(a-b)(a-c)(a-d)\dots(b-c)(b-d)\dots$$

Dieses Product muss bei jeder Transposition das Zeichen wechseln. Sind nämlich p und q zwei Buchstaben, r ein dritter Buchstabe, so kommen im Producte die beiden Factoren $\pm(p-r)$ und $\pm(q-r)$ vor, deren Product durch die Transposition $(p\,q)$ unverändert bleibt.

Die Factoren wechseln also immer paarweise das Zeichen; hiervon ist $p-q$ ausgenommen, welches in $q-p$ übergeht, und folglich wechselt das ganze Product durch die Transposition das Zeichen. Falls nun das Product der Transpositionen 1 ist, so wird man nach Ausführung aller Transpositionen zu dem ursprünglichen Product zurückgekehrt sein; die Anzahl der Transpositionen muss deshalb gerade sein.

Wie man auch eine Substitution in Transpositionen zerlegen möge, die Anzahl derselben wird immer gerade oder ungerade sein.

Man nehme an, dass ein Product von m Transpositionen gleich einem Producte von n Transpositionen sei; multiplicirt man nach und nach mit den m Transpositionen, mit einer zur Zeit, auf beiden Seiten des Gleichheitszeichens, so erhält man ein Prodnct von $m+n$ Transpositionen, welches gleich 1 ist; $m+n$ ist also eine gerade Zahl; m und n sind deshalb beide gerade oder beide ungerade Zahlen.

Dadurch wird man darauf geführt, die Substitutionen in zwei Klassen zu theilen, nämlich in solche, welche aus einer geraden, und in solche, welche aus einer ungeraden Anzahl Transpositionen bestehen. Nennt man die der ersten Art *positiv,* die der zweiten *negativ,* so wird das Vorzeichen eines Productes auf gewöhnliche Weise bestimmt, so dass es negativ wird, wenn es eine ungerade Anzahl negativer Substitutionen enthält. Man sieht leicht, dass eine cyclische Substitution positiv ist, wenn sie eine ungerade, negativ wenn

sie eine gerade Anzahl Buchstaben hat. Falls eine Substitution μ Cyclen mit beziehungsweise n_1, $n_2 \ldots n_\mu$ Buchstaben hat, wird ihr Zeichen

$$(-1)^{n_1 + n_2 \cdots + n_\mu - \mu},$$

so dass also der Unterschied zwischen der Anzahl der Buchstaben und der Anzahl der Cyclen gerade oder ungerade ist, je nachdem die Substitution positiv oder negativ ist.

Zweites Kapitel.

Conjugirte Substitutionen oder Gruppen.

Satz von Lagrange.

158. Ein System von Substitutionen, welches die Eigenschaft hat, dass man aus denselben durch Multiplication nicht neue Substitutionen bilden kann, heisst ein conjugirtes System oder eine *Gruppe*. So werden z. B. alle Potenzen einer beliebigen Substitution eine Gruppe bilden; dasselbe gilt von allen $n!$ Substitutionen, welche aus n Buchstaben gebildet werden können (die vollständige Gruppe). Dass die Gruppe G aus den Substitutionen $1, S_1, S_2 \ldots$ besteht, wird folgendermassen bezeichnet:

$$G = (1, S_1, S_2 \ldots).$$

Die Anzahl der Substitutionen in einer Gruppe heisst die *Ordnung* der Gruppe, die Anzahl der Buchstaben, welche vorkommen, der *Grad* derselben; die Ordnung einer Substitution ist also gleich der Ordnung der Gruppe, welche die Potenzen derselben bilden.

159. *Wenn eine Gruppe Γ von der Ordnung μ mit enthalten ist in einer Gruppe G von der Ordnung m, so muss μ ein Divisor von m sein.* (Satz von Lagrange.)

Die erste Gruppe Γ möge aus den Substitionen

$$1, S_1, S_2, \dots S_{\mu-1}$$

bestehen, und T_1 sei eine andere von den Substitutionen in G; dann müssen in G auch

$$T_1, S_1 T_1, S_2 T_1, \dots S_{\mu-1} T_1$$

vorkommmen; sind mehr Substitutionen in G enthalten, z. B. T_2, so müssen auch

$$T_2, S_1 T_2, S_2 T_2, \dots S_{\mu-1} T_2$$

vorkommen und so weiter; fährt man fort, bis man alle in G vorkommenden Substitutionen mitbekommen hat, so erhält man diese in einer gewissen Anzahl Reihen, und zwar μ in jeder Reihe, angeordnet; der Satz ist deshalb bewiesen, wenn alle Substitutionen, welche in den Reihen vorkommen, verschieden sind; im entgegesetzten Falle müsste indessen

$$S_\alpha T_\beta = S_{\alpha_1} T_{\beta_1}$$

für gewisse Werthe von α, β, α_1 und β_1 sein; es sei nun $\beta > \beta_1$; dann erhielte man

$$T_\beta = S_\alpha^{-1} S_{\alpha_1} T_{\beta_1},$$

was unmöglich ist, da die Substitution auf der rechten Seite in der Reihe

$$T_{\beta_1}, S_1 T_{\beta_1}, \dots S_{\mu-1} T_{\beta_1}$$

vorkommt, und T_β gerade eine Substitution ist, welche nicht in dieser oder in einer der vorhergehenden Reihen vorkommt.

Der Factor T ist hier auf der rechten Seite der Factoren S hinzugesetzt worden; auf ähnliche Weise kann man die Substitutionen der Gruppe in Reihen von der Form

$$T_\alpha, T_\alpha S_1, T_\alpha S_2 \dots T_\alpha S_{\mu-1}$$

anordnen. Aus dem soeben bewiesenen wichtigen Satze lassen sich leicht folgende ableiten:

Die Ordnung einer Gruppe vom Grade n ist ein Divisor von n!. Die Gruppe ist nämlich in der vollständigen Gruppe mitenthalten.

Die Ordnung einer Gruppe ist durch die Ordnung einer jeden Substitution der Gruppe theilbar.

Die Gruppe enthält nämlich die Gruppe, welche aus den Potenzen der Substitution gebildet wird.

Eine Gruppe, deren Ordnung eine Primzahl p ist, enthält nur regelmässige Substitutionen von der Ordnung p (ausser der Substitution 1). *Ist der Grad auch p, so besteht die Gruppe aus den p Potenzen einer cyclischen Substitution von der Ordnung p.*

Ferner sieht man leicht:

Die Substitutionen, welche zwei Gruppen gemeinschaftlich sind, bilden selber eine Gruppe.

Das Product zwei solcher Substitutionen muss sich nämlich in beiden Gruppen finden und gehört also auch zu den gemeinschaftlichen Substitutionen.

Diejenigen Substitutionen einer Gruppe, welche nicht gewisse Buchstaben versetzen, bilden selber eine Gruppe.

Wenn nämlich gewisse Buchstaben nicht von zwei Substitutionen versetzt werden, können sie auch nicht dadurch versetzt werden, dass man diese Substitutionen nach einander anwendet.

Alle Substitutionen einer Gruppe, welche gegen eine gewisse Substitution vertauscht werden können, bilden selber eine Gruppe.

Substitutionen, welche mit einer Gruppe permutabel sind.

160. *Wenn alle Substitutionen einer Gruppe G,*

$$1, S_1, S_2, \ldots S_{m-1},$$

durch eine gewisse Substitution T transformirt werden, so erhält man wieder eine Gruppe.

Man hat nämlich

$$T S_1 T^{-1} . T S_2 T^{-1} = T (S_1 S_2) T^{-1}.$$

Die Substitutionen der beiden Gruppen sind paarweise ähnlich und die Gruppen selber werden *ähnlich* genannt.

Wenn die transformirte Gruppe mit der gegebenen Gruppe übereinstimmt, so sagt man, dass die Substitution T mit der Gruppe G *permutabel* sei; in diesem Falle hat man für jedes α

$$T S_\alpha = S_\beta T$$

für einen gewissen Werth von β.

Alle Substitutionen einer Gruppe G, welche mit einer Gruppe H permutabel sind, bilden selber eine Gruppe; man hat nämlich, wenn U und T mit $H = (1, S_1, S_2, \ldots)$ permutabel sind,

$$U T S_\alpha (U T)^{-1} = U T S_\alpha T^{-1} U^{-1} = U S_\beta U^{-1} = S_\gamma,$$

so dass U T unter den Substitutionen vorkommt, wenn U und T dort vorkommen.

161. Eine Gruppe heisst *einfach,* wenn sie keine andere Gruppe enthält, mit welcher alle ihre Substitutionen permutabel sind; im entgegengesetzten Fall heisst sie *zusammengesetzt.*

G sei eine zusammengesetzte Gruppe, welche die Gruppe H enthält, mit welcher alle ihre Substitutionen permutabel sind; H bestehe aus den Substitutionen

$$1, S_1, S_2 \dots S_{m-1}.$$

T sei eine Substitution von G, welche sich nicht unter den Substitutionen S findet; Potenzen von T können möglicherweise in H vorkommen; T^α sei die niedrigste von diesen. Alle Substitutionen von der Form

$$T^\beta S_k$$

finden sich in G und sind verschieden für $\beta < \alpha$; für $\beta = \alpha$ erhält man H, und für $\beta > \alpha$ erhält man periodisch dieselbe Reihe von Substitutionen wie früher, in der Weise dass man jedesmal H bekommt, wenn β ein Vielfaches von α wird; die Ordnung von T muss deshalb ein Vielfaches von α sein.

Die αm Substitutionen, welche gebildet worden sind, bilden eine Gruppe H_1, denn man sieht leicht, dass das Product von zweien derselben eine Substitution giebt, welche unter den αm Substitutionen vorkommt, wenn man bedenkt, dass für einen passenden Werth von h

$$T^\beta S_k = S_h T^\beta.$$

Ueber die Bildung einiger verschiedener Gruppen.

162. *Alle Substitutionen, welche eine Substitution T in eine Potenz von T transformiren, bilden eine Gruppe.*

Hat man nämlich, wenn α und β prim zu μ (der Ordnung von T) sind,

$$M T M^{-1} = T^\alpha; \; N T N^{-1} = T^\beta,$$

so hat man auch

$$(M N) T (M N)^{-1} = M N T N^{-1} M^{-1} = M T^{\beta} M^{-1}$$
$$= M T M^{-1} M T M^{-1} \ldots = T^{\alpha\beta},$$

so dass MN unter den betrachteten Substitutionen vorkommt, wenn M und N dort vorkommen.

Ferner geht hieraus hervor, dass man auch eine Gruppe erhält, wenn man aus den Substitionen der gefundenen Gruppe nur solche entnimmt, *bei denen die Exponenten von T eine gewisse Bedingung erfüllen,* wenn diese derartig ist, dass $\alpha\beta$ dieselbe erfüllt, sobald α und β es thun ($\alpha\beta$ nach dem Modulus μ genommen); dies gilt, wenn α und β prim zu μ sind, aber auch, wenn α und β nur solche Zahlen, prim zu μ, sind, welche die Congruenz

$$x^{\theta} \equiv k^{m} \pmod{\mu},$$

worin θ und k gegebene Zahlen sind (k prim zu μ) befriedigen, während m unbestimmt ist; aus

$$\alpha^{\theta} \equiv k^{m_1}; \; \beta^{\theta} \equiv k^{m_2}$$

folgt nämlich

$$(\alpha\beta)^{\theta} \equiv k^{m_1 + m_2}.$$

Man betrachte z. B. eine cyclische Substitution T mit μ Buchstaben und wähle für α und β alle Zahlen, welche prim zu μ sind; die Anzahl dieser sei $\varphi(\mu)$; aus T werden dann $\varphi(\mu)$ Potenzen gebildet, und jede von diesen kann aus T durch Transformation mit μ verschiedenen Substitutionen gebildet werden, da jeder Buchstabe der Potenz vorangestellt werden kann. Hierdurch erhält man also eine Gruppe von $\mu\,\varphi(\mu)$ Substitutionen; ist $\mu = p$ eine Primzahl, so wird die Ordnung $p(p-1)$. Man könnte sich auch damit begnügen die Substitutionen zu betrachten, welche man erhält, wenn T und die Potenzen davon so geschrieben werden, dass sie mit demselben Buchstaben anfangen; dieser Buchstabe kommt dann nicht mit in die gesuchten Substitutionen, und diese

bilden eine Gruppe mit $\mu - 1$ Buchstaben von der Ordnung $\varphi(\mu)$.

Beisp. 1.

$$T = (a\,b\,c\,d\,e\,f);$$
$$T^5 = (a\,f\,e\,d\,c\,b).$$

Die Transformation geschieht durch

$$M = \begin{pmatrix} a\,f\,e\,d\,c\,b \\ a\,b\,c\,d\,e\,f \end{pmatrix} = (b\,f)\,(c\,e),$$

welche in Verbindung mit 1 eine Gruppe zweiter Ordnung bildet. Wird T^5 auf alle Arten geschrieben, so erhält man eine Gruppe zwölfter Ordnung, welche die vorige mit in sich fasst.

Beisp. 2.

$$T = (a\,b\,c\,d\,e);$$
$$T^2 = (a\,c\,e\,b\,d);$$
$$T^3 = (a\,d\,b\,e\,c);$$
$$T^4 = (a\,e\,d\,c\,b).$$

Soll a bei der Transformation seinen Platz behalten, so erhält man die Gruppe vierter Ordnung

$$1,\ (b\,c\,e\,d),\ (b\,d\,e\,c),\ (b\,e)\,(c\,d).$$

Es wurde gezeigt, dass man, wenn μ eine Primzahl p war, eine Gruppe mit $p-1$ Buchstaben von der Ordnung $p-1$ erhielt; diese Gruppe muss aus Potenzen einer cyclischen Substitution von der Ordnung $p-1$ bestehen, sobald eine solche in der Gruppe vorkommt; nun kann man indessen

$$T = (a_0\,a_1\,a_2 \ldots a_{p-1});\ T^r = (a_0\,a_r\,a_{2r} \ldots)$$

setzen, wodurch man die Transformante

$$U = \begin{pmatrix} a_0\,a_r\,a_{2r} \ldots \\ a_0\,a_1\,a_2 \ldots \end{pmatrix} = (a_1\,a_r\,a_{r^2} \ldots)$$

erhält, welche cyclisch wird, wenn r eine primitive Wurzel

von p ist. Da nun jede Primzahl primitive Wurzeln hat, wird die gesuchte Gruppe

$$1,\ U,\ U^2 \dots U^{p-2}.$$

Will man die Gruppe bilden, deren Ordnung $p(p-1)$ ist, so schreibt man T^r mit jedem Buchstaben zu Anfang; die Transformanten haben dann alle die Form

$$T^h U^k, \dots\dots\dots\dots \quad (1)$$

indem man durch Transformation mit U^k die gewünschte Potenz von T erhält, anfangend mit a_0, und darauf durch Transformation durch T^h einen anderen Buchstaben auf den ersten Platz bringt; ist also z. B.

$$T = (a\,b\,c\,d\,e);\ T^3 = (b\,e\,c\,a\,d),$$

so erhält man die Transformante

$$\begin{pmatrix} b\,e\,c\,a\,d \\ a\,b\,c\,d\,e \end{pmatrix} = \begin{pmatrix} b\,e\,c\,a\,d \\ a\,d\,b\,e\,c \end{pmatrix} \begin{pmatrix} a\,d\,b\,e\,c \\ a\,b\,c\,d\,e \end{pmatrix} = T\,(b\,d\,e\,c).$$

Man erhält also die gesuchte Gruppe, indem man alle Potenzen von U links mit allen Potenzen von T multiplicirt; multiplicirt man rechts, so erhält man dieselben Substitutionen in einer anderen Reihenfolge.

Die alterne Gruppe.

163. *Von den $N = n!$ Substitutionen, welche aus n Buchstaben gebildet werden können, bilden die positiven eine Gruppe von der Ordnung $\frac{1}{2} N$, und es giebt keine andere Gruppe von derselben Ordnung.*

Falls eine Gruppe eine negative Substitution enthält, muss sie ebenso viele negative wie positive enthalten; denn multiplicirt man alle Substitutionen der Gruppe mit einer

von den negativen, so erhält man dieselbe Gruppe wieder; da nun durch diese Multiplication alle Substitutionen von negativen zu positiven übergehen und umgekehrt, müssen gleich viele von jeder Art vorhanden sein. Wie leicht ersichtlich bilden die positiven für sich eine Gruppe; also bilden alle möglichen positiven Substitutionen eine Gruppe von der Ordnung $\frac{1}{2}N$; diese heisst die alterne Gruppe.

Man nehme an, dass man eine Gruppe von der Ordnung $\frac{1}{2}N$ und mit den Substitutionen $1, S_1, S_2 \ldots$ habe. T sei eine Substitution, die unter diesen nicht vorkommt; die $\frac{1}{2}N$ Substitutionen von der Form TS sind dann alle unter sich und von den Substitutionen S verschieden. Da die Substitutionen S und TS ihrer Zahl nach N sind, so dass man unter ihnen alle Substitutionen findet, müssen die Substitutionen $T^2 S$ mit den Substitutionen S übereinstimmen, und dasselbe gilt von $T^4 S$, $T^6 S$ u. s. w. T muss deshalb von gerader Ordnung sein, da man im entgegengesetzten Falle TS in der gegebenen Gruppe antreffen müsste. Diese enthält deshalb alle cyclischen Substitutionen dritter Ordnung und ist folglich die alterne Gruppe, denn man hat

$$(a_1 a_2)(a_2 a_3) = (a_1 a_2 a_3); \quad (a_1 a_2)(a_3 a_4) = (a_1 a_2 a_3)(a_2 a_3 a_4)$$

so dass jede positive Substitution als ein Product von cyclischen Substitutionen dritter Ordnung dargestellt werden kann.

Eine Function, welche, ohne symmetrisch zu sein, nicht durch Substitutionen der alternen Gruppe verändert wird, heisst *alternirend*. Eine solche Function hat nur zwei Werthe, da jede Substitution die Form S oder TS hat, wenn S zu der alternen Gruppe gehört und T eine gegebene negative Substitution ist; da nun die Function nicht durch S verändert wird, erhält sie nur den einen neuen Werth, welchen T ihr verleiht. Eine solche Function ist z. B.

$$y = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1),$$

welche nur die beiden Werthe y und $-y$ hat.

164. *Eine Gruppe, welche alle cyclischen Substitutionen dritter Ordnung enthält, ist entweder die alterne oder die vollständige Gruppe.*

Es wurde nämlich oben (163) gezeigt, dass eine solche Gruppe alle positiven Substitutionen enthält.

Eine Gruppe, welche alle cyclischen Substitutionen p^{ter} Ordnung enthält, ist entweder die alterne oder die vollständige Gruppe.

Man hat nämlich

$$(a_1\, a_2\, a_3) = (a_1\, a_3\, a_4\, a_2\, a_5 \ldots a_p)\, (a_p\, a_{p-1} \ldots a_5\, a_2\, a_1\, a_4\, a_3),$$

so dass die Gruppe alle cyclischen Substitutionen dritter Ordnung enthält.

Gruppen, welche aus anderen Gruppen durch Multiplication gebildet werden.

165. Wenn zwei Gruppen

$$1,\ S_1,\ S_2,\ \ldots S_{m-1};$$

$$1,\ T_1,\ T_2,\ \ldots T_{n-1}$$

die Eigenschaft haben, dass

$$S_\alpha T_\beta = T_{\beta_1} S_{\alpha_1}$$

für alle Werthe von α und β und passende Werthe von α_1 und β_1, so sagt man, dass die Gruppen vertauscht werden können.

Multiplicirt man alle Substitutionen S mit allen Substitutionen T (auf derselben Seite), so erhält man eine neue Gruppe von der Ordnung m n, falls die gegebenen Gruppen keine anderen Substitutionen als 1 gemeinschaftlich haben.

Die Substitutionen, welche man erhält, sind nämlich alle verschieden, denn aus

$$S_\alpha T_\beta = S_{\alpha_1} T_{\beta_1}$$

würde

$$S_{\alpha_1}^{-1} S_\alpha = T_{\beta_1} T_\beta^{-1}$$

folgen, und das würde mit sich bringen, dass die beiden gegebenen Gruppen eine Substitution, die nicht 1 sein kann, gemeinschaftlich hätten; ferner kann

$$S_\alpha T_\beta S_{\alpha_1} T_{\beta_1}$$

durch Vertauschung der Factoren und die daraus folgende Veränderung der Indices auf die Form

$$S_\gamma T_\delta$$

gebracht werden, woraus hervorgeht, dass die $m\,n$ Substitutionen eine Gruppe bilden.

Man sieht leicht, wie der Satz formulirt werden muss, wenn man mehrere Gruppen betrachtet.

Cauchy's Sätze.

166. *Wenn p eine Primzahl ist, kann man immer aus k Buchstaben eine Gruppe bilden, deren Ordnung die höchste Potenz von p ist, welche in k! aufgeht.*

Für $k < p$ wird die Gruppe 1 von der Ordnung p^0 die angegebene Eigenschaft besitzen; man braucht also nur zu beweisen, dass der Satz für alle Zahlen bis $p^{\alpha+1}$ gilt, wenn er für alle Zahlen bis p^α gilt.

Eine Zahl zwischen p^α und $p^{\alpha+1}$ kann durch $p\,q + r$ ausgedrückt werden, wo $q < p^\alpha$ und $r < p$; es wird also vorausgesetzt, dass man aus den q Buchstaben a, b, c ... eine Gruppe

von der Ordnung p^β bilden könne, wo p^β die höchste Potenz von p ist, welche in q! aufgeht. Aus jeder Substitution $(a\,b\,c\ldots)(d\,e\ldots)\ldots$ dieser Gruppe bilde man eine andere

$$(a_1\,b_1\,c_1\ldots)(a_2\,b_2\,c_2\ldots)\ldots(a_p\,b_p\,c_p\ldots)\ldots(d_1\,e_1\ldots)$$
$$(d_2\,e_2\ldots)(d_p\,e_p\ldots)\ldots;$$

indem man jeden Cyclus durch ein Product von p Cyclen mit denselben Buchstaben, versehen mit den Indices $1, 2\ldots p$, ersetzt. Die auf solche Weise gebildeten Substitutionen bilden eine Gruppe vom Grade pq und der Ordnung p^β; diese Gruppe möge durch

$$T = (C_1, C_2, \ldots)$$

bezeichnet werden; die Substitutionen derselben vertauschen die Buchstaben ohne die Indices zu verändern.

Nun mögen die cyclischen Substitutionen

$$(a_1\,a_2\ldots a_p), (b_1\,b_2\ldots b_p)\ldots$$

durch

$$S_a, S_b\ldots$$

bezeichnet werden; dieselben vertauschen die Indices ohne die Buchstaben zu verändern. Die gesuchte Gruppe besteht nun aus allen Substitutionen von der Form

$$S_a^\gamma S_b^\delta \ldots C_\mu,$$

und es ist die Anzahl derselben $p^q \cdot p^\beta$. Es lässt sich beweisen, dass alle diese Substitutionen verschieden sind und dass sie eine Gruppe bilden; man hat nämlich, wenn C_μ b durch a ablöst,

$$S_a^\gamma C_\mu = C_\mu S_b^\gamma,$$

da beide Substitutionen b_k durch $a_{k+\gamma}$ ablösen; man kann also die Factoren in einem Producte S C vertauschen, wenn

man gleichzeitig den Index von S auf passende Weise verändert; wenn nun z. B.

$$S_a^\gamma S_b^\delta \ldots C_\mu = S_c^\varepsilon S_d^\eta \ldots C_\gamma,$$

so muss ein C, welches nur Buchstaben vertauscht, durch ein Product von Substitutionen S, welche nur Indices vertauschen, ausgedrückt werden können. Da dies unmöglich ist, müssen die $p^{q+\beta}$ Substitutionen alle verschieden sein; sie bilden ferner eine Gruppe, denn in dem Producte von zweien derselben kann man auf die oben angegebene Weise die eine Substitution C nach rechts rücken, bis sie hin zu der anderen gebracht ist; das Product erhält dann dieselbe Form wie die Factoren und gehört zu den $p^{q+\beta}$ Substitutionen.

Es erübrigt noch, die höchste Potenz von p zu suchen, welche in $(pq+r)!$ aufgeht; unterdrückt man die Factoren, welche nicht durch p theilbar sind, so erhält man $p^q . q!$; nach der Voraussetzung ist p^β indessen die höchste Potenz, welche in $q!$ aufgeht; also ist $p^{\beta+q}$ die höchste Potenz, welche in $(pq+r)!$ aufgeht, und diese Zahl war eben die, welche die Ordnung der oben gebildeten Gruppe angab.

167. *Wenn die Gruppe G, von der Ordnung g, die beiden Gruppen H und K, von den Ordnungen h und k, enthält, und wenn in H keine Substitution (1 ausgenommen) vorkommt, welche einer Substitution in K ähnlich ist, so muss hk in g aufgehen.*

Die Substitutionen i H mögen durch S, die in K durch T und beliebige Substitutionen in G durch U bezeichnet werden; man kann dann hk Substitutionen von G von der Form

$$S_\alpha U_1 T_\beta$$

bilden; diese sind alle verschieden, da

$$S_\alpha U_1 T_\beta = S_{\alpha_1} U_1 T_{\beta_1}$$

mit sich führen würde, dass

$$U_1 T_\beta T_{\beta_1}^{-1} U_1^{-1} = S_\alpha^{-1} S_{\alpha_1};$$

das ist aber unmöglich, da $T_\beta T_{\beta_1}^{-1}$ und $S_\alpha^{-1} S_{\alpha_1}$ nicht beide 1 sein können und nicht ähnlich sind.

Nun sei U_2 eine Substitution, welche unter den hk soeben gebildeten Substitutionen nicht vorkommt; G muss dann auch alle hk verschiedenen Substitutionen von der Form $S_\alpha U_2 T_\beta$ enthalten und diese müssen von den vorigen verschieden sein, da

$$S_\alpha U_1 T_\beta = S_{\alpha_1} U_2 T_{\beta_1}$$

mit sich führen würde, dass U_2 unter den früher gebildeten Substitutionen vorkäme; fährt man nun auf diese Weise so lange fort, als es eine Substitution U giebt, welche noch nicht berücksichtigt ist, so erhält man alle Substitutionen in G in Reihen angeordnet, und zwar hk Substitutionen in jeder Reihe. hk geht deshalb in g auf.

168. *Eine Gruppe G, deren Ordnung durch eine Primzahl p theilbar ist, muss eine Substitution von der Ordnung p enthalten.*

Die Gruppe enthalte k Buchstaben und sei von der Ordnung g; diese und die oben (166) gebildete Gruppe Γ von der Ordnung p^β sind beide in der vollständigen Gruppe von der Ordnung $k!$ enthalten. Falls G keine Substitution von der Ordnung p enthält, hat sie keine Substitution, welche einer Substitution in Γ ähnlich ist, denn Γ enthält nur Substitutionen, deren Ordnung eine Potenz von p ist (159), und es giebt immer Potenzen von den diesen ähnlichen Substitutionen, deren Ordnung p ist; es müsste also $k!$ theilbar sein durch $g p^\beta$ (167), aber das ist unmöglich, wenn g den Primfactor p enthält, denn p^β ist die höchste Potenz von p, welche in $k!$ aufgeht; es muss deshalb in G wenigstens eine Substitution von der Ordnung p sein.

Transitive und intransitive Gruppen.

169. Eine Gruppe heisst *transitiv,* wenn man durch ihre Substitutionen einen beliebigen Buchstaben dahin bringen kann, einen beliebigen der übrigen Buchstaben abzulösen; sie heisst dagegen *intransitiv,* wenn dieses nicht der Fall ist.

Wenn die Gruppe intransitiv ist, und a_1 die Buchstaben $a_2, a_3, \ldots a_p$, nicht aber $b_1, b_2, \ldots b_q$ ablösen kann, so kann überhaupt kein Buchstabe a einen Buchstaben b ablösen; im entgegengesetzten Fall könnte man nämlich, durch Combinirung zweier Substitutionen, a_1 dahin bringen einen Buchstaben b abzulösen. Bei den intransitiven Gruppen können deshalb die Buchstaben in zwei oder mehrere solche Systeme getheilt werden, dass jeder Buchstabe nur Buchstaben desselben Systems ablösen und nur von Buchstaben desselben Systems abgelöst werden kann; jede Substitution muss deshalb aus Cyclen bestehen, welche jeder nur Buchstaben enthalten, die demselben System angehören.

Natürlich muss man festhalten, welche Buchstaben vorliegen; so ist z. B. die vollständige Gruppe von $n-1$ Buchstaben transitiv, wenn man es nur mit diesen $n-1$ Buchstaben zu thun hat, aber sie ist intransitiv, sobald man es mit mehr Buchstaben zu thun hat, da die übrigen dann nicht versetzt werden.

Eine Gruppe heisst m mal transitiv, wenn dieselbe m beliebige Buchstaben durch m beliebige andere, die von den ersten verschieden oder nicht verschieden sind, ablösen kann. Wenn dieselbe m beliebige durch m bestimmte Buchstaben ablösen kann, so sieht man leicht, dass sie dieselben auch durch m beliebige ablösen kann.

Die vollständige Gruppe von n Buchstaben ist $(n-1)$ mal transitiv, die alterne Gruppe ist $(n-2)$ mal transitiv. Enthält eine Gruppe von n Buchstaben eine cyclische Substitution von n Buchstaben, so ist sie wenigstens einmal transitiv; enthält sie ausserdem eine cyclische Substitution von $n-1$ Buchstaben, so ist sie wenigstens zweimal transitiv u. s. w.

170. *Wenn man aus einer Gruppe G (transitiv oder intransitiv) gewisse Buchstaben a, b, c... herausnimmt, und wenn die besondere Gruppe H, welche diese Buchstaben nicht versetzt, von der Ovdnung k ist, so ist G von der Ordnung kp, wo p die Anzahl der Systeme von Plätzen ist, welche a, b, c... durch G's Substitutionen einzunehmen im Stande sind.*

H möge nämlich aus den Substitutionen

$$1, T_1, T_2, \dots T_{k-1}$$

bestehen, während R eine der übrigen Substitutionen ist; alle Substitutionen

$$R, T_1 R, T_2 R, \dots T_{k-1} R$$

bringen dann die Buchstaben a, b, c... auf denselben Platz, und das gilt nur von diesen Substitutionen; falls nämlich R_1 sie auf denselben Platz bringen würde, müsste $R_1 R^{-1}$ sie auf ihrem ursprünglichen Platz stehen lassen und deshalb zu den Substitutionen T gehören. R_1 muss deshalb unter den Substitutionen TR vorkommen. Die Substitutionen in G können deshalb in p Reihen mit k in jeder Reihe angeordnet werden.

Ist G m mal transitiv, und nimmt man m Buchstaben a, b, c... heraus, so wird, wenn die Anzahl der Buchstaben n ist,

$$p = n(n-1)\dots(n-m+1);$$

man ersieht hieraus, dass *die Ordnung einer m mal transitiven Gruppe von n Buchstaben durch $n(n-1)\dots(n-m+1)$ theilbar ist.*

Ist G intransitiv, und nimmt man ein System von α Buchstaben heraus, welche unter einander vertauscht werden, so bilden die Substitutionen, welche diese nicht vertauschen, eine Gruppe von einer gewissen Ordnung k; die Anzahl der Plätze, auf welche die α Buchstaben gebracht werden können, ist ein Divisor von $\alpha!$. Die Ordnung von G ist also ein Divisor von $k . \alpha!$; behandelt man nun die $n - \alpha$ Buchstaben

auf dieselbe Weise u. s. w., so sieht man, dass die Ordnung von G ein Divisor von $\alpha!\,\beta!\,\gamma!\ldots$ ist, wo α, β, $\gamma\ldots$ die Anzahl der Buchstaben in den verschiedenen Systemen angiebt, und wo also

$$\alpha+\beta+\gamma\ldots=n.$$

171. *Wenn eine Gruppe m mal transitiv ist und eine Substitution enthält, welche nicht mehr als m Buchstaben versetzt, so muss die Gruppe die alterne oder die vollständige Gruppe sein.*

S sei die Substitution, welche höchstens m Buchstaben versetzt, S_1 eine beliebige dieser ähnliche Substitution; die Gruppe muss eine Substitution enthalten, welche die Buchstaben in S durch die entsprechenden Buchstaben in S_1 ablöst (169); wird S durch diese Substitution transformirt, so erhält man S_1, welche Substitution deshalb auch in der Gruppe vorkommen muss.

Nun sei einer der Cyclen in S

$$(a_1\, a_2\, a_3 \ldots a_p);$$

für S_1 kann man dann eine Substitution nehmen, unter deren Cyclen sich

$$(a_p\, a_{p-1} \ldots a_4\, a_2\, a_3\, a_1)$$

befindet, während die übrigen Cyclen in S_1 dieselben sind wie die in S, mit den Buchstaben in umgekehrter Reihenfolge. G enthält dann auch

$$S_1 S = (a_1\, a_3\, a_2)$$

und also alle cyclischen Substitutionen dritter Ordnung. G enthält also die alterne Gruppe (164).

Der Beweis setzt voraus, dass in S ein Cyclus mit wenigstens drei Buchstaben vorkommt; im entgegengesetzten Fall kann man für die beiden Cyclen von S und S_1

$$(a_1\, a_2) \text{ und } (a_2\, a_3)$$

nehmen, wo a_3 eine Buchstabe ist, der nicht in S vorkommt; hierdurch erhält man $S_1 S_2 = (a_1 a_2 a_3)$.

172. *Wenn eine Gruppe m mal transitiv ist und eine Substitution enthält, welche nicht mehr als 2m — 4 Buchstaben versetzt, so muss die Gruppe die alterne oder die vollständige Gruppe sein.*

Es sei nämlich

$$S = (a b c \ldots)(d e f \ldots)(g \ldots)$$

eine der Substitutionen, welche q Buchstaben versetzt, wo $m < q < 2m - 3$. Die Gruppe enthält eine Substitution T, welche nicht die $m - 1$ von diesen Buchstaben $a b c \ldots d e$ versetzt und die übrigen durch Buchstaben $\alpha \beta \gamma \ldots$ ablöst, von welchen wenigstens einer, α, welcher f ablöst, nicht unter den q Buchstaben vorkommt. Die Gruppe enthält dann auch die Substition

$$U = T S T^{-1} = (a b c \ldots)(d e \alpha \ldots)(\beta \ldots) \ldots$$

zugleich mit der Substitution $S^{-1} U$, welche nur die Buchstaben e, α, β, f, g ... enthält und nicht 1 sein kann, da sie in jedem Falle α versetzt; die Anzahl ihrer Buchstaben ist höchstens

$$2(q - m + 1) + 1 = 2q - 2m + 3 < q;$$

auf diese Weise wurde mit Hülfe der gegebenen Substitution eine andere gefunden, welche weniger Buchstaben versetzt; fährt man auf dieselbe Weise fort, so findet man zuletzt eine Substitution, welche höchstens m Buchstaben versetzt, und damit ist der Satz bewiesen.

Die Anzahl Buchstaben, welche von der die wenigsten Buchstaben versetzenden Substitution einer Gruppe versetzt wird, heisst *die Klasse der Gruppe.*

173. *Die Ordnung einer Gruppe mit n Buchstaben, welche m mal transitiv ist und die alterne Gruppe nicht enthält, ist ein Divisor von*

$$\frac{n!}{\alpha!},$$

wo α die grösste von den Zahlen m und 2m — 4 ist.

Bildet man nämlich die vollständige Gruppe von α Buchstaben, so enthält diese keine Substitution, welche einer Substitution der gegebenen Gruppe, deren Substitutionen alle mehr als α Buchstaben versetzen, ähnlich ist; ist die Ordnung dieser g, so muss deshalb $g \cdot \alpha!$ ein Factor von $n!$ sein (167).

174. *Eine Gruppe vom Grade n, welche die alterne Gruppe nicht enthält, kann nicht mehr als q mal transitiv sein, wo q die kleinste der Zahlen*

$$\frac{n+4}{3} \text{ und } \frac{n}{2}$$

bedeutet.

Wenn die Gruppe q mal transitiv ist, so ist ihre Ordnung ein Vielfaches (170) von

$$n(n-1)\dots(n-q+1);$$

diese Zahl muss also in $\frac{n!}{\alpha!}$ aufgehen (173), oder $(n-q)!$ muss theilbar sein durch $\alpha!$; man muss also haben

$$n-q \geqq \alpha; \; q \leqq n-\alpha,$$

wo α die grösste der Zahlen q und $2q-4$ ist; hieraus folgt beziehungsweise

$$q \leqq \frac{n}{2} \text{ und } q \leqq \frac{n+4}{3}.$$

Jordan hat gezeigt, dass eine Gruppe vom Grade $p+\alpha$ nicht mehr als α mal transitiv sein kann, wenn p eine Primzahl ist und $\alpha > 2$. (Bulletin de la soc. math. de France I.)

175. *Wenn eine n mal transitive Gruppe G eine Gruppe H enthält, welche mit den sämmtlichen Substitutionen von G permutabel ist, so ist G wenigstens (n — 1) mal transitiv.* (Hiervon eine Ausnahme.)

Der Satz gilt für $n=2$, denn ist $S=(a\,b\dots)(\dots)\dots$ eine Substitution von H, so wird G eine Substitution T enthalten, welche a und b durch zwei beliebige Buchstaben

ablöst, und H wird dann $T S T^{-1}$ enthalten, welche einen beliebigen Buchstaben durch einen beliebigen Buchstaben ablöst.

Aus den Gruppen G und H bilde man im allgemeinen Falle zwei neue Gruppen G_1 und H_1, indem man alle Substitutionen entfernt, welche einen der Buchstaben, z. B. a, enthalten; H_1 ist dann in G_1 enthalten und mit allen Substitutionen von G_1 permutabel. Da G n mal transitiv ist, muss G_1 $(n-1)$ mal transitiv sein.

H ist wenigstens einmal mehr transitiv als H_1, denn durch eine der entfernten Substitutionen kann man a einen willkürlichen Platz einnehmen lassen. Der Satz gilt also für G und H, wenn er für G_1 und H_1 gültig ist. Da nun der Satz für $n = 2$ bewiesen ist, gilt er für alle n, wenn nur nicht eine der successiv gebildeten Gruppen H_1 nur die identische Substitution 1 enthält.

Man hat also den Fall $H_1 = (1)$ näher zu betrachten; in diesem Falle müssen alle Substitutionen von H (die Substitution 1 ausgenommen) alle die in G vorkommenden Buchstaben enthalten, denn sonst könnte man für a einen der fehlenden Buchstaben wählen; nur eine der Substitutionen kann a durch b ablösen; sind nämlich T und U zwei verschiedene Substitutionen, welche beide a durch b ablösen, muss $T U^{-1}$ von 1 verschieden sein und kann a nicht enthalten. Andererseits wird a von allen übrigen Buchstaben abgelöst, woraus folgt, dass die Anzahl der Substitutionen mit der Anzahl der Buchstaben übereinstimmt. Hieraus folgt, dass H einmal transitiv ist (170).

Ist G nun zweimal transitiv, so gilt der Satz; man hat also nur den Fall $n > 2$ zu betrachten.

Fände sich nun in H ein Substitution

$$S = (a\, b\, c \ldots)(\ldots),$$

müsste auch eine andere Substitution

$$S_1 = (a\, b\, d \ldots)(\ldots)$$

sich dort finden, denn da G mehr als zweimal transitiv ist,

kommt unter deren Substitutionen eine vor, welche S in S_1 transformirt. Die Cyclen von den Substitutionen in H können also nur zwei Buchstaben enthalten; ebenso ersieht man, dass man nur $n = 3$ haben kann.

Da alle Substitutionen von H von der zweiten Ordnung sind, ist die Ordnung von H eine Potenz von 2. Alle Substitutionen der Gruppe H sind vertauschbar; sind nämlich S und T zwei solche, hat man

$$(S\,T)\,(S\,T) = 1 \text{ woraus } S\,T = T\,S.$$

Die in der vollständigen Gruppe vierter Ordnung enthaltene Gruppe

$$1,\ (a\,b)\,(c\,d),\ (a\,c)\,(b\,d),\ (a\,d)\,(b\,c)$$

bietet ein Beispiel dar.

Ueber transitive Gruppen, welche transitive Untergruppen enthalten.

176. G sei eine transitive Gruppe von höherem als dem p^{ten} Grade, welche eine m mal transitive Untergruppe A mit den Buchstaben $a_1, a_2, \ldots a_p$ enthält; es wird vorausgesetzt, dass weder G noch irgend welche Untergruppe mehr als m mal transitiv sei.

Die übrigen Buchstaben in G seien $b_1, b_2 \ldots$; in G kommt eine Substitution vor, welche ein beliebiges a, z. B a_k durch b_1 ablöst. Wenn nicht noch andere Buchstaben b in dieser Substitution vorkämen, würde man b_1 durch T auf einen beliebigen Platz und darauf durch A m Buchstaben a auf beliebige Plätze bringen können; G würde dann eine $(m + 1)$ mal transitive Gruppe enthalten, und da dieses den Voraussetzungen widerstreitet, muss mehr als ein b in T vorkommen.

Wenn die Substitution T, welche ein a durch ein b ablöst, z. B. a_1 durch b_1, nicht jedes a durch ein b ablöst, sondern z. B. a_k durch a_l, so hat man

$$T = \begin{pmatrix} b_1 & a_l & b_2 & \dots \\ a_1 & a_k & \alpha & \dots \end{pmatrix},$$

wo α ein b oder ein a sein kann. Die Substitution T, welche hier betrachtet wird, möge die sein, welche die kleinste Anzahl von Buchstaben b enthält.

Bedeutet nun α ein b, also z. B.

$$T = \begin{pmatrix} b_1 & a_l & b_2 & \dots \\ a_1 & a_k & b_q & \dots \end{pmatrix},$$

so nehme man in der Gruppe A eine Substitution S, welche a_1 durch a_k ablöst; die Substitution

$$T S T^{-1} = (b_1 a_l \dots)(\dots)\dots$$

löst dann ein b durch ein a ab und enthält nicht b_2. Das ist unmöglich, da T so wenig Buchstaben b wie möglich enthält.

Bedeutet α ein a, so hat man z. B.

$$T = \begin{pmatrix} b_1 & a_l & b_2 & \dots \\ a_1 & a_k & a_r & \dots \end{pmatrix}.$$

Ist nun A wenigstens zweimal transitiv, so kommt in A eine Substitution S vor, welche a_1 nicht versetzt und a_r an Stelle von a_k setzt; man hat dann

$$T S T^{-1} = (a_l b_2 \dots)(\dots)\dots,$$

worin b_1 nicht vorkommt. Da auch dieses den Voraussetzungen widerstreitet, so kann, für $m > 1$, keine Substitution von G ein a durch ein b ablösen, ohne zugleich jedes a durch ein b abzulösen; es müssen deshalb in G wenigstens p Buchstaben b vorkommen.

In T mögen $a_1, a_2 \dots a_p$ durch $b_1, b_2 \dots b_p$ abgelöst werden. Transformirt man A durch T, so erhält man eine

m mal transitive Gruppe B von b_1, $b_2 \dots b_p$; sind mehr Buchstaben vorhanden, so mögen sie durch c_1, $c_2 \dots$ bezeichnet werden. Eine Substitution U, welche ein a durch ein c ablöst, muss jedes a durch ein c ablösen. Nimmt man nämlich an, dass a_1 von c_1, a_2 von b_2 abgelöst wird, und ist S eine Substitution der Gruppe A, welche a_2 durch a_1 ablöst, so wird

$$U S U^{-1}$$

kein a versetzen und wird b_2 durch c_1 ablösen, aber nicht jedes b durch ein c. Das ist indessen unmöglich, denn die Gruppe G enthält B und die Substitution $U S U^{-1}$, welche kein a versetzt, und ein b kann dann nur durch ein c abgelöst werden, wenn jedes b durch ein c abgelöst wird. Es müssen also wenigstens p Buchstaben c vorkommen, und eine m mal transitive Gruppe C, welche nur diese Buchstaben unter einander vertauscht, kann durch Transformation von A gefunden werden.

Fährt man auf dieselbe Weise fort, so sieht man, dass die in G vorkommenden Buchstaben Systeme bilden, jedes von p Buchstaben, nämlich a, b, c... mit den Indices 1, 2...p. Die Substitutionen vertauschen die Buchstaben desselben Systems unter einander oder lösen gleichzeitig alle Buchstaben eines Systems durch die Buchstaben eines anderen Systems ab.

Solche Gruppen heissen *imprimitiv* im Gegensatz zu *primitiven* Gruppen, deren Buchstaben nicht in solche Systeme zerfallen. Die imprimitiven Gruppen sind nur einmal transitiv, da sie z. B. nicht a_1 und b_1 durch a_2 und a_3 ablösen können.

177. Es wurde vorausgesetzt, dass die Gruppe A wenigstens zweimal transitiv sei; ist sie nur einmal transitiv, so kann die Substitution T, welche am wenigsten Buchstaben b enthält, die Buchstaben a theils durch verschiedene a, theils durch verschiedene b ablösen; angenommen es sei

$$T = \begin{pmatrix} b_1\, b_2\, b_3 \dots a_\gamma\, a_\delta \dots \\ a_1\, a_2\, a_3 \dots a_\alpha\, a_\beta \dots \end{pmatrix}.$$

Wenn nun eine Substitution S der Gruppe A, z. B. a_1 durch a_2 und a_3 durch a_α ablöst, wird $T^{-1}ST$ b_2 durch b_1 und a_γ durch b_3 ablösen; es ist nachgewiesen, dass dies unmöglich sei, falls nicht jedes a durch ein b abgelöst wird; es muss deshalb unter den Buchstaben a ein solches System vorkommen, dass A nur diese Buchstaben unter einander vertauschen kann oder alle dieselben durch die übrigen Buchstaben a ablösen muss.

Aus einer wenigstens zweimal transitiven Gruppe vom p^{ten} Grade können also durch Hinzufügung neuer Buchstaben nur neue Gruppen gebildet werden, indem man entweder einen Buchstaben zur Zeit hinzufügt und dadurch Gruppen erhält, welche jede einmal mehr transitiv sind als vorher, oder indem man Systeme von p Buchstaben hinzufügt und dadurch eine imprimitive Gruppe bildet. Dasselbe gilt, wenn A einmal transitiv ist, wenn nur nicht in A ein System von Buchstaben vorkommt, welche nur unter einander vertauscht oder gleichzeitig alle von anderen abgelöst werden.

Besonders sind zwei specielle Fälle zu beachten:

Eine transitive Gruppe n^{ten} Grades, welche eine cyclische Substitution der p^{ten} Ordnung enthält, wo p eine Primzahl $> \frac{n}{2}$, ist wenigstens $(n - p + 1)$ mal transitiv.

Eine transitive Gruppe, welche eine alterne Untergruppe enthält, ist imprimitiv, oder auch enthält sie die alterne Gruppe aller Buchstaben (170).

178. *Ordnung imprimitiver Gruppen.* In der imprimitiven Gruppe G mit den m p Buchstaben $a_1, a_2, \ldots a_p$; $b_1, b_2, \ldots b_p$; $c_1, c_2, \ldots c_p$; ... können Buchstaben desselben Systems nur Buchstaben desselben Systems ablösen. Es seien nun T_1 und T_1' zwei solche Substitutionen, welche dieselben Buchstaben a, b, c ... in derselben Reihenfolge vertauschen, während $S_1, S_2 \ldots$ die Substitutionen bezeichnen mögen, welche nur Indices versetzen. Die Substitution $T'_1 T_1^{-1}$ muss dann zu den Substitutionen S gehören; in der Reihe

$$T_1, S_1 T_1, S_2 T_1 \ldots$$

kommen dann alle diejenigen Substitutionen von G vor, welche, ohne Rücksicht auf die Indices, dieselben Buchstaben einander ablösen lassen. Es sei

$$U_1 = (a\,b\,c\ldots)(d\,e\ldots)$$

eine Substitution, deren Buchstaben a, b, c ... eben einander auf dieselbe Weise ablösen.

Aus einer anderen Substitution von G, welche nicht zu den Substitutionen S oder $S\,T_1$ gehört, bilde man nun auf dieselbe Weise die Reihe

$$T_2,\ S_1\,T_2,\ S_2\,T_2\ldots,$$

welche durch die Substitution U_2 characterisirt wird u. s. w.

Die Substitutionen U bilden eine Gruppe; kommt nämlich $T_\alpha\,T_\beta$ in der Reihe vor, welche mit T_γ beginnt, so muss

$$U_\alpha\,U_\beta = U_\gamma$$

sein.

Die Ordnung von G ist also ein Divisor von

$$m!\,(p!)^m,$$

da G mit einbegriffen ist in der imprimitiven Gruppe, für welche U die vollständige Gruppe von der Ordnung m! ist, und S_1, S_2 ... durch Multiplication aus den m vollständigen Gruppen der m Systeme von Buchstaben gebildet sind.

Eine Gruppe H wird *isomorph* mit einer Gruppe K genannt, wenn jede Substitution in K einer Substitution in H entspricht, und jede Substitution in H einer oder mehreren Substitutionen in K entspricht, während zugleich das Product von zwei Substitutionen in K dem Producte der entsprechenden Substitutionen in H entspricht. Nach dieser Definition und nach dem, was oben gezeigt worden, ist also die Gruppe U isomorph mit der Gruppe G.

Beisp. Nimmt man

$$U_1 = 1, \ U_2 = (a\,b), \ p = 2,$$

so kann man folgende Gruppe vom vierten Grade und der achten Ordnung bilden:

$$1, (a_1 a_2), (b_1 b_2), (a_1 a_2)(b_1 b_2),$$
$$(a_1 b_1 a_2 b_2), (a_1 b_1)(a_2 b_2), (a_1 b_2)(a_2 b_1), (a_1 b_2 a_2 b_1).$$

Diese Gruppe ist imprimitiv und isomorph mit der Gruppe 1, (a b).

Gruppe einer Function und Anzahl der Werthe derselben.

179. *Die Substitutionen, welche auf eine gegebene Function angewendet werden können ohne dieselbe zu verändern, bilden eine Gruppe.*

Wird nämlich die Function durch die Substitutionen S und T nicht verändert, so kann sie auch dadurch nicht verändert werden, dass man diese beiden Substitutionen nach einander anwendet; die Substitution S T muss deshalb unter den Substitutionen vorkommen, welche die Function nicht verändern, und diese bilden also eine Gruppe; diese heisst die *Gruppe der Function,* und man sagt, dass die Function die Substitutionen der Gruppe *zulasse;* ist die Function z. B. symmetrisch, so wird ihre Gruppe die vollständige Gruppe, ist sie alternirend, so wird es die alterne. Die oben betrachtete Gruppe von der Ordnung 8 und dem Grade 4 (178) gehört zu den Functionen (a_1 ist durch x_1 ersetzt u. s. w.)

$$(x_1 + x_2)(x_3 + x_4), \ x_1 x_2 + x_3 x_4, \ (x_1 - x_2 + x_3 - x_4)^2 \text{ u. s. w.}$$

Nun sei die Gruppe einer Function von der Ordnung g, und bestehe aus den Substitutionen

$$1, S_1, S_2, \ldots S_{g-1}.$$

Die vollständige Gruppe kann dann, wenn die Anzahl der Buchstaben n ist, in $\frac{n!}{g}$ Reihen von der Form

$$T_\alpha, T_\alpha S_1, T_\alpha S_2, \ldots T_\alpha S_{g-1}$$

angeordnet werden.

Da nun die Substitutionen S die Function nicht verändern, werden alle Substitutionen in einer solchen Reihe der Function denselben Werth geben, welchen T_α ihr verleiht. *Man erhält deshalb die Anzahl der Werthe einer Function mit n Buchstaben, wenn man n! durch die Ordnung der Gruppe der Function dividirt.*

Beisp. Die drei Werthe

$$x_1 x_2 + x_3 x_4, x_1 x_3 + x_2 x_4, x_1 x_4 + x_2 x_3$$

werden demgemäss aus dem ersten durch die Substitutionen

$$1, (x_2 x_3), (x_2 x_4)$$

gebildet.

Die Gruppe der Function besteht aus 8 Substitutionen; werden diese mit den drei hier gefundenen multiplicirt, so erhält man die 24 Substitutionen der vollständigen Gruppe. Das Product oder die Summe der drei Werthe der Function wird durch keine der 24 Substitutionen verändert und ist deshalb symmetrisch.

180. Es lässt sich immer eine Function bilden, welche eine gewisse gegebene Gruppe hat; man kann nämlich eine Function y bilden, welche lauter verschiedene Werthe hat, z. B.

$$y = \alpha_1 x_1 + \alpha_2 x_2 + \ldots,$$

wo α_1, $\alpha_2 \ldots$ verschiedene Zahlen sind; diese Function möge durch die Substitutionen der gegebenen Gruppe die Werthe $y_1, y_2 \ldots$ annehmen. Man sieht dann leicht, dass

$$z = (\alpha - y_1)(\alpha - y_2) \ldots,$$

worin α unbestimmt ist, nicht verändert wird durch alle Substitutionen der gegebenen Gruppe, während sie durch alle übrigen verändert wird.

181. *Wenn die Gruppe G der Function y_0 angehört, und diese durch eine andere Substitution T zu y_1 wird, so wird die Gruppe, welche y_1 angehört, diejenige sein, welche aus G mittelst Transformation durch T gebildet wird.*

S sei nämlich eine Substitution in G; S verändert dann nicht y_0; $T S T^{-1}$ wird dann y_1 nicht verändern; man hat nämlich $T y_0 = y_1$, oder $T^{-1} y_1 = y_0$; also ist

$$T S T^{-1} y_1 = T S y_0 = T y_0 = y_1.$$

Falls G mit T permutabel ist, stimmt die transformirte Gruppe mit G überein, so dass diese Gruppe sowohl y_0 als auch y_1 angehört. Auf die Weise sieht man, dass *die Gruppe G, sobald sie y_0 angehört, auch allen Functionen angehört, welche aus y_0 durch Substitutionen gebildet werden, welche mit G permutabel sind.*

Index einer Gruppe.

182. Unter dem *Index* einer Gruppe versteht man die Zahl, welche man erhält, wenn man die Ordnung der vollständigen Gruppe durch die Ordnung der Gruppe dividirt.

Bildet man eine Function, welche nicht durch alle Substitutionen der Gruppe, wohl aber durch alle übrigen Substitutionen verändert wird, so wird die Anzahl der Werthe der Function, nach dem was oben (179) gezeigt worden, genau gleich dem Index der Gruppe sein. Die vollständige Gruppe hat zum Index 1, die alterne 2.

Es wurde oben (170) gefunden, dass die Ordnung einer intransitiven Gruppe mit n Buchstaben ein Divisor von

$\alpha!\,\beta!\ldots$ sei, worin $\alpha+\beta\ldots=n$. Der Index der Gruppe ist also ein Vielfaches von

$$\frac{n!}{\alpha!\,\beta!\ldots}.$$

Die Ordnung einer imprimitiven Gruppe ist zufolge 170 ein Divisor von

$$m!\,(p!)^m,$$

wenn die Gruppe m Systeme von p Buchstaben enthält; der kleinstmögliche Werth für den Index i ist deshalb

$$i=\frac{mp\,(mp-1)\ldots(m+1)}{2.3\ldots p.2.3\ldots p\ldots 2.3.p},$$

wo Zähler und Nenner gleich viel Factoren enthalten. Für $n=4$ erhält man die Gruppe des Beispiels in 178 mit dem Index 3; für $n=6$ wird der kleinste Index 10, für $n=8$ wird er 35 und so fort, stark wachsend; auf eine genauere Untersuchung dieses Falles wird hier verzichtet, aber es wird als evident vorausgesetzt, dass der hier bestimmte Index für $n>4$ in jedem Falle grösser als n ist.

183. Es erübrigt noch eine primitive Gruppe zu betrachten, welche keine alterne Gruppe enthält. $p_1, p_2\ldots$ seien verschiedene Primzahlen, deren Summe nicht grösser sein möge als die Anzahl n der verschiedenen Buchstaben; man bilde dann aus p_1 Buchstaben eine cyclische Substitution, welche nicht in der Gruppe vorkommt; nicht alle cyclischen Substitutionen der übriggebliebenen Buchstaben von der Ordnung p_1 können in der Gruppe vorkommen; man nehme dann eine solche, welche nicht vorkommt; auf solche Weise verfahre man so lange wie möglich; T sei die Substitution von der Ordnung $p_1\,p_2\ldots$, welche man erhält, wenn man die gebildeten cyclischen Substitutionen mit einander multiplicirt.

Weder T noch die Potenzen von T können in der Gruppe vorkommen, denn diese müsste dann auch die

Potenzen der darin vorkommenden Substitution enthalten, und unter diesen findet sich wenigstens eine von den cyclischen Substitutionen, welche nicht vorkommen.

Nun seien 1, S_1, S_2 ... die Substitutionen der gegebenen Gruppe, und ihre Anzahl sei q; man bilde dann alle Substitutionen von der Form $T^\alpha S_\beta$; diese sind alle verschieden und ihre Anzahl ist $q\, p_1\, p_2 \dots$ Diese Anzahl kann indessen n! nicht übersteigen; also ist

$$q \leqq \frac{n!}{p_1 p_2 \cdots}; \; i \geqq p_1 p_2 \cdots$$

Hieraus ersieht man, dass *der Index nicht kleiner sein kann als das grösste Product verschiedener Primzahlen, deren Summe n nicht übersteigt.*

184. Die gebrauchten Primzahlen seien $p_1, p_2, \dots p_\alpha$; dann ist

$$p_1 + p_2 + \dots + p_\alpha \leqq n,$$

aber

$$p_1 + p_2 + \dots + p_\alpha + p_\beta > n,$$

wo p_β eine beliebige neue Primzahl ist; nun ist die Zahl

$$p_1 p_2 \cdots p_{\alpha-1} - p_\alpha,$$

wo p_α die grösste (oder jedenfalls die nächstgrösste) von diesen Primzahlen ist, nicht theilbar durch irgend eine von den Primzahlen $p_1, p_2, \dots p_\alpha$; sie ist deshalb eine neue Primzahl oder ein Product von solchen; p_β kann deshalb so gewählt werden, dass sie nicht grösser ist als diese Zahl, und man hat dann

$$p_1 + p_2 + \dots + p_{\alpha-1} + p_1 p_2 \cdots p_{\alpha-1} > n,$$

oder

$$i \geqq p_1 p_2 \cdots p_{\alpha-1} p_\alpha > \frac{1}{2} p_\alpha n.$$

Auf solche Weise ist ersichtlich, dass es nur eine Gruppe giebt, deren Index grösser als 1 und kleiner als n ist, nämlich für $n = 4$. Von Gruppen aus n Buchstaben, deren Index n ist, hat man zunächst die vollständige Gruppe von $n - 1$ Buchstaben. Diese Gruppe gehört Functionen von n Grössen an, welche mit Beziehung auf $n - 1$ derselben symmetrisch sind. Nimmt man oben für $p_1\, p_2 \ldots$ die Primzahlen 2, 3, 5 ..., so sieht man, dass eine Gruppe mit dem Index n hier nur möglich ist für $n < 10\, (= 2 + 3 + 5)$; da nun $9 = 7 + 2$; $8 = 3 + 5$; $7 = 2 + 5$; $5 = 2 + 3$, so erübrigt nur die Untersuchung für den Fall, wo $n = 4$ und $n = 6$. Man sieht leicht, dass es für $n = 4$ keine transitive Gruppe mit dem Index 4 giebt; für $n = 6$ giebt es dagegen eine Gruppe mit dem Index 6; dieselbe ist dreimal transitiv und gehört Functionen an, welche 6 Werthe haben, ohne mit Beziehung auf 5 derselben symmetrisch zu sein; eine solche Function ist z. B. das Product der folgenden 5 Grössen:

$$ab + cd + ef,\ ac + be + fd,\ ad + bf + ce,$$

$$ae + bd + fc,\ af + bc + ed.$$

Es ist also unmöglich eine Function von n Buchstaben zu bilden, welche mehr als zwei und weniger als n Werthe hat, ausser für $n = 4$, oder eine Function zu bilden, welche n Werthe hat, ohne mit Beziehung auf $n - 1$ Buchstaben symmetrisch zu sein, ausser für $n = 6$.

Die linearen Substitutionen.

185. Eine Substitution sei aus den Buchstaben $a_0, a_1 \ldots a_{n-1}$ gebildet; wird bei der Erwähnung der Indices der Buchstaben eine Zahl grösser als $n - 1$ genannt, so ist darunter der Rest zu verstehen, den sie bei der Division durch n giebt. α, $n + \alpha$, $2n + \alpha \ldots$ bezeichnen also alle denselben Index.

Nun bezeichne

$$\binom{F(z)}{z}$$

die Substitution, welche einen beliebigen Buchstaben mit dem Index z durch den Buchstaben ablöst, welcher den Index F(z) hat. Die Function F muss also so beschaffen sein, dass sie für $z = 0, 1, 2 \ldots n-1$ dieselben Werthe, nur in anderer Reihenfolge, erhält.

Hier sollen im Besonderen die *linearen* Substitutionen

$$\binom{az+b}{z}$$

betrachtet werden; $F(z) = az + b$ genügt der gestellten Bedingung, wenn man für b eine beliebige Zahl und für a eine Zahl wählt, die prim zu n ist; man sieht nämlich leicht, dass man in diesem Falle lauter verschiedene Reste erhält, wenn z alle seine Werthe annimmt.

Unter die gewählte Bezeichnung fallen die cyclischen Substitutionen; so hat man z. B. für

$$S = (a_0\, a_1\, a_2 \ldots a_{n-1})$$

$$S = \binom{z+1}{z};\ S^2 = \binom{z+2}{z};\ S^3 = \binom{z+3}{z} \ldots \text{ u. s. w.}$$

$$\binom{2z}{z} = (a_1\, a_2\, a_4\, a_8 \ldots);\ \binom{2z+1}{z} = (a_0\, a_1\, a_3\, a_7 \ldots) \text{ u. s. w.}$$

Die Anzahl linearer Substitutionen von n Buchstaben ist $n\varphi(n)$, wo $\varphi(n)$ die Anzahl der Zahlen bedeutet, welche kleiner als n und prim zu n sind; a kann nämlich $\varphi(n)$ und b kann n verschiedene Werthe haben. Alle diese Substitutionen bilden eine Gruppe; denn das Product von zweien giebt wieder eine derselben; man hat nämlich

$$\binom{cz+d}{z}\binom{az+b}{z} = \binom{acz+ad+b}{z}.$$

Diese Gruppe ist genau dieselbe, welche früher (162) gebildet wurde, denn transformirt man

$$(a_0\, a_1\, a_2 \ldots)$$

durch

$$\binom{az+b}{z},$$

so erhält man eine Substitution, bei der die Reihe der Indices

$$b,\ a+b,\ 2a+b,\ \ldots$$

ist, so dass die Substitution in ihre a^{te} Potenz transformirt ist.

Aus der vorstehenden Entwicklung zieht man leicht den Schluss, dass alle Substitutionen in der linearen Gruppe durch Multiplication der beiden

$$\binom{z+1}{z} \text{ und } \binom{az}{z},$$

wo a eine beliebige Zahl, prim zu n, bedeutet, gebildet werden können.

186. *Ist $n = p$, und bedeutet p eine Primzahl, so wird die Ordnung der Gruppe $p(p-1)$, und es lässt sich aus p Buchstaben keine andere Gruppe derselben Ordnung bilden.*

Zufolge des Satzes von Cauchy (168) muss nämlich eine Gruppe von der Ordnung $p(p-1)$ eine cyclische Substitution von der Ordnung p enthalten; diese und ihre Potenzen seien

$$1,\ S,\ S^2,\ \ldots S^{p-1}$$

während T eine der übrigen Substitutionen der Gruppe bezeichnet; alle Substitutionen von der Form

$$S^\alpha\, T\, S^\beta$$

können nicht verschieden sein, da ihre Anzahl p^2 ist; für gewisse Werthe der Exponenten muss also

$$S^\alpha\, T\, S^\beta = S^\gamma\, T\, S^\delta$$

sein, oder

$$T S^{\beta-\delta} T^{-1} = S^{\gamma-\alpha};$$

durch Potenziren erhält man hieraus

$$T S T^{-1} = S^{m}.$$

Die Substitutionen T können deshalb nur solche sein, durch welche die Substitution S in ihre Potenzen transformirt wird, und diese Substitutionen bilden eben, wie oben bewiesen worden, die lineare Gruppe.

187. Der Begriff lineare Substitution lässt sich auch auf gebrochene Substitutionen ausdehnen, so dass

$$F(z) = \frac{az + b}{a_1 z + b_1};$$

unter $F(z) = q$ hat man dann den Werth von q zu verstehen, welcher durch die unbestimmte Gleichung (es wird nur der Fall $n = p$ in Betracht gezogen)

$$az + b = q(a_1 z + b_1) + yp$$

bestimmt wird; für den Werth von z, welcher $a_1 z + b_1$ zu einem Vielfachen von p macht, erhält man indessen $q = \infty$; man muss deshalb einen Buchstaben mit dem Index ∞ hinzufügen, so dass die Substitution $p + 1$ Buchstaben

$$a_0, a_1 \ldots a_{p-1}, a_\infty$$

enthält. Der Buchstabe a_∞ wird dann von dem Buchstaben a_α abgelöst, der durch

$$\alpha \equiv \frac{a}{a_1} \text{ oder } \alpha a_1 + yp = a$$

bestimmt wird.

Die Substitutionen bilden eine Gruppe von der Ordnung $(p-1)p(p+1)$; die genauere Untersuchung mag hier übergangen werden.

Man hat gleichfalls den Begriff dadurch erweitert, dass man jeden Buchstaben mit mehreren Indices, z. B. x und y, versah.

Durch

$$\begin{pmatrix} x, & ax + by \\ y, & a_1 x + b_1 y \end{pmatrix}$$

oder

$$\begin{pmatrix} ax + by & a_1 x + b_1 y \\ x & y \end{pmatrix}$$

wird dann die Substitution bezeichnet, welche den Buchstaben

$$a_{x,y} \text{ durch } a_{ax+by,\, a_1x+b_1y}$$

ablöst; die Indices sind hier wie oben als Reste bei der Division durch einen gewissen Divisor zu verstehen; dies findet namentlich dann Anwendung, wenn die Anzahl der Buchstaben, welche versetzt werden, eine Potenz von einer Primzahl ist. Für den Modulus p repräsentirt nämlich z. B. $a_{x,y,z}$ genau p^3 verschiedene Buchstaben.

Unter »der linearen Gruppe« versteht man im Allgemeinen die vollständige lineare Gruppe von der Ordnung $n\varphi(n)$; doch nennt man auch kleinere hierin enthaltene transitive Gruppen linear; die Ordnung derselben ist αn, wo α einen Divisor von $\varphi(n)$ bedeutet.

Drittes Kapitel.

Theorie von Galois.

Gruppe einer Gleichung.

188. Eine irreductible Gleichung kann reductibel werden, wenn man übereinkommt, dass Vorkommen gewisser irrationaler Grössen in den Coefficienten der Gleichungen zu gestatten, in welche die gegebene zerlegt wird. So ist z. B. die Gleichung

$$x^2 - 4x + 1 = 0$$

irreductibel; sie wird aber reductibel wenn man $\sqrt{3}$ benutzen darf, denn dann zerfällt sie in die beiden

$$x - 2 + \sqrt{3} = 0 \text{ und } x - 2 - \sqrt{3} = 0;$$

von einer Grösse, welche auf diese Weise benutzt wird, sagt man, dass sie der Gleichung *adjungirt* sei. Die angeführte Gleichung ist also reductibel, wenn man $\sqrt{3}$ adjungirt, hingegen irreductibel, wenn man $\sqrt{5}$, $\sqrt{7}$ u. s. w. adjungirt. Jede Gleichung wird reductibel, wenn eine oder mehrere ihrer Wurzeln adjungirt werden.

Im Folgenden wird vorausgesetzt, dass eine oder mehrere irrationale Grössen den Gleichungen, welche behandelt werden,

adjungirt sein können; diese Grössen können dann auch in rationaler Weise in die Coefficienten der Gleichung eintreten.

Galois hat gezeigt, dass jeder Gleichung eine gewisse Gruppe von Substitutionen entspricht, welche für die Gleichung characteristisch ist oder richtiger für eine Klasse von Gleichungen, zu welcher die gegebene gehört. Wenn man eine gewisse für die Gleichung eigenthümliche Eigenschaft der Wurzeln kennt, kann man diese benutzen, um die Gruppe der Gleichung zu finden. Umgekehrt kann man, wenn man die Gruppe kennt, aus dieser Eigenschaften für die Klasse von Gleichungen, welche diese Gruppe hat, ableiten. Es soll nun gezeigt werden, wie man zu der Gruppe einer Gleichung gelangt.

189. Die gegebene Gleichung n^{ten} Grades, reductibel oder irreductibel, aber jedenfalls *ohne gleiche Wurzeln,* sei

$$f(x) = 0 \quad \dots\dots\dots\dots\dots \quad (1)$$

mit den Wurzeln

$$x_1, x_2, \dots x_n;$$

man bilde dann eine Function der Wurzeln, welche lauter *numerisch* verschiedene Werthe hat, wenn alle möglichen Substitutionen auf die Function angewendet werden; dieselbe hat dann $n!$ Werthe und wird durch eine Gleichung vom Grade $n!$ ohne gleiche Wurzeln bestimmt; man kann z. B. die Function

$$y_1 = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n \quad \dots\dots\dots \quad (2)$$

benutzen, in der $\alpha_1, \alpha_2, \alpha_3 \dots$ so gewählt sind, dass alle Werthe von y verschiedene Zahlenwerthe haben.

Die Gleichung vom Grade $n!$, welche alle Werthe von y bestimmt, ist möglicherweise reductibel; man zerlege sie dann in irreductible Gleichungen und bezeichne eine derselben vom Grade m (die *Resolvente* der gegebenen Gleichung) durch

$$F(y) = 0, \quad \dots\dots\dots\dots\dots \quad (3)$$

die Wurzeln derselben durch

$$y_1, y_2, \dots y_m.$$

Es ist bewiesen worden, dass jede dieser Wurzeln als eine rationale Function einer beliebigen der übrigen Wurzel ausgedrückt werden kann (74); ferner ist bewiesen worden (73), dass jede Wurzel der Gleichung (1) als eine rationale Function von jeder Wurzel der Gleichung (3) ausgedrückt werden kann.

Nun mögen die Wurzeln der Gleichung (1), in einer gewissen Reihenfolge genommen, dem entsprechend durch

$$\Psi_1 (y_1), \Psi_2 (y_1) \dots \Psi_n (y_1) \dots\dots\dots\dots (4)$$

ausgedrückt werden, wo $\Psi_1, \Psi_2, \dots \Psi_n$ rationale Functionen sind. Die Permutation der Wurzeln, welche hier vorliegt, werde mit A_1 bezeichnet; vertauscht man y_1 mit einer anderen Wurzel von (3), z. B. mit y_k, so geht (4) in eine andere Permutation A_k von $x_1, x_2 \dots$ über, nämlich in diejenige, welche aus A_1 durch dieselbe Substitution gebildet wird, durch welche y_k aus y_1 gebildet wird (75).

Auf diese Weise erhält man m Permutationen von $x_1, x_2 \dots x_n$, nämlich

$$A_1, A_2, \dots A_m; \dots\dots\dots\dots\dots (5)$$

diese werden alle aus A_1 durch gewisse Substitutionen gebildet, welche mit

$$1, S_1, S_2, \dots S_{m-1} \dots\dots\dots\dots (6)$$

bezeichnet werden mögen; *von diesen kann man beweisen, dass sie eine Gruppe bilden.*

Man hat nämlich

$$y_k = \theta (y_1),$$

wo θ eine gewisse rationale Function bedeutet; es kann also

die Reihe A_k oder $S_{k-1} A_1$ (wenn man θy_1 anstatt $\theta(y_1)$ schreibt u. s. w.) ausgedrückt werden durch

$$\Psi_1 \theta y_1, \Psi_2 \theta y_1, \ldots \Psi_n \theta y_1,$$

und man erhält dann, wenn man hierauf S_{q-1} anwendet, für die Reihe $S_{q-1} S_{k-1} A_1$

$$\Psi_1 \theta y_q, \Psi_2 \theta y_q \ldots \Psi_n \theta y_q,$$

da S_{q-1} ausgeführt wird, wenn man y_q an Stelle von y_1 setzt.

Falls nun diese Reihe von Wurzeln mit einer von den Reihen A übereinstimmt, wird das Product $S_{q-1} S_{k-1}$ unter den Substitutionen (6) vorkommen und diese werden deshalb eine Gruppe bilden.

Da nun inzwischen $\theta(y_1) = y_k$ eine Wurzel der irreductiblen Gleichung (3) ist, muss die Gleichung vom Grade m, deren Wurzeln $\theta(y_1)$, $\theta(y_2) \ldots \theta(y_m)$ sind, mit (3) übereinstimmen, und es muss dann z. B.

$$\theta(y_q) = y_r$$

sein, woraus man ersieht, dass die Reihe oben mit der Reihe A_r übereinstimmt.

Dergestalt ist bewiesen, dass die m Substitutionen (6) eine Gruppe bilden; es ist diejenige, welche Galois die Gruppe der gegebenen Gleichung genannt hat; dieselbe möge durch G bezeichnet werden.

Haupteigenschaften der Gruppe einer Gleichung.

190. *Jede rationale Function U der Wurzeln, deren numerischer Werth nicht durch die Substitutionen in G verändert wird, kann rational durch bekannte Grössen ausgedrückt werden.*

Die Function U kann nämlich rational durch eine der Wurzeln von (3), z. B. y_1, ausgedrückt werden, so dass also

$$U = \varphi(y_1),$$

wo φ eine rationale Function bedeutet.

Da nun die Substitutionen in G den Werth von U nicht verändern, und diese Substitutionen dadurch ausgeführt werden können, dass man y_1 mit y_2, $y_3 \dots y_m$ vertauscht, so hat man auch

$$U = \varphi(y_2) = \varphi(y_3) \dots = \varphi(y_m),$$

folglich

$$U = \frac{1}{m}\left(\varphi(y_1) + \varphi(y_2) \dots + \varphi(y_m)\right).$$

U ist auf diese Weise als eine symmetrische Function der Wurzeln der Gleichung (3) ausgedrückt und kann deshalb rational durch bekannte Grössen ausgedrückt werden.

191. *Eine rationale Function der Wurzeln, welche rational durch bekannte Grössen ausgedrückt werden kann, muss ihren numerischen Werth unverändert behalten, wenn die Substitutionen der Gruppe G darauf angewendet werden.*

Der gegebene Werth der Function sei B; man hat dann, wenn die Wurzeln, welche in der gegebenen Function vorkommen, alle durch y_1 ausgedrückt werden,

$$\varphi(y_1) = B,$$

wo φ eine rationale Function bedeutet; y_1 ist also eine Wurzel der Gleichung

$$\varphi(y) - B = 0,$$

welche folglich auch die Wurzeln y_2, y_3, $\dots y_m$ haben muss; man hat deshalb

$$\varphi(y_2) = B;\ \varphi(y_3) = B \dots \varphi(y_m) = B,$$

so dass die gegebene Function den Werth B bei allen Substitutionen in G behält.

Man sieht übrigens, dass der Beweis seine Gültigkeit behält, selbst wenn B irrational ist, wenn nur (3) durch die Adjungirung dieser Grösse fortfährt irreductibel zu sein.

192. *Keine Substitution, welche nicht G angehört, kann jede Function der Wurzeln, deren Werth rational ist, unverändert lassen.*

Betrachtet man nämlich die Function

$$(\alpha - y_1)(\alpha - y_2)\dots(\alpha - y_m),$$

wo α beliebig ist, so sieht man leicht, dass diese Function, deren Werth rational ist, nur durch die Substitutionen unverändert bleiben kann, welche $y_1, y_2 \dots y_m$ unter einander vertauschen, also durch die Substitutionen von G. Hieraus folgt, dass eine Gleichung nur eine Gruppe haben kann; *man muss deshalb zu dieser gelangen, welche von den mit (3) analogen Gleichungen man auch benutzen mag.* Diese sind deshalb alle von demselben Grade.

193. *Sind zwei rationale Functionen der Wurzeln, φ und Ψ, gleich gross, so müssen sie fortfahren es zu sein, nachdem man eine der Substitutionen in G an ihnen ausgeführt hat.* Ihre Differenz ist nämlich rational und muss deshalb ihren Werth Null bei jeder solchen Substitution behalten.

194. *Die Gruppe G ist transitiv oder intransitiv, je nachdem die Gleichung irreductibel oder reductibel ist.*

Falls die Gruppe intransitiv ist, vertauscht sie gewisse Wurzeln unter einander, ohne sie mit den übrigen zu vertauschen; sie verändert deshalb nicht eine beliebige symmetrische Function dieser Wurzeln, und eine solche Function kann dann rational ausgedrückt werden; diese Wurzeln werden deshalb durch eine Gleichung mit rationalen Coefficienten bestimmt, und die gegebene Gleichung ist folglich reductibel.

Falls andererseits die Gleichung reductibel ist, muss man für gewisse Wurzeln

$$(\alpha - x_1)(\alpha - x_2)\dots(\alpha - x_p) = K$$

haben, wo α beliebig und K rational ist; dieses Product kann den Werth K nur für solche Substitutionen behalten, welche nur $x_1, x_2, \dots x_p$ unter einander vertauschen, oder welche diese Wurzeln garnicht versetzen; G kann deshalb nur solche Substitutionen enthalten und ist also intransitiv.

Behält man von den Substitutionen in G nur die Cyclen, welche $x_1, x_2 \dots x_p$ enthalten, so gelangt man zu einer Gruppe G_1. Eine Function dieser Wurzeln, welche nicht von G_1 verändert wird, aber von allen anderen Substitutionen, welche $x_1, x_2 \dots x_p$ versetzen, hat einen rationalen Werth, da sie nicht von G verändert wird. G_1 gehört also zu der Gleichung mit den Wurzeln $x_1, x_2 \dots x_p$.

195. *Die Gleichung, welche durch Elimination von y aus*

$$y^m + a_1 y^{m-1} + \dots a_m = 0$$

und

$$\varphi_0(y) x^n + \varphi_1(y) x^{n-1} + \dots \varphi_n(y) = 0$$

gebildet wird, wo $a_1, a_2 \dots$ rational und $\varphi_0, \varphi_1 \dots$ rationale Functionen sind, hat eine imprimitive Gruppe, und umgekehrt wird jede Gleichung, deren Gruppe imprimitiv ist, durch eine solche Elimination gebildet werden können.

Die Wurzeln der ersten Gleichung seien $y_1, y_2 \dots y_m$, während die zweite Gleichung, wenn man y_ρ statt y setzt die Wurzeln $x_{\rho,1}, x_{\rho,2} \dots x_{\rho,n}$ haben mögen.

Nun sei v_ρ eine beliebige symmetrische Function dieser n Wurzeln; die Function

$$A = (\alpha - v_1)(\alpha - v_2)\dots(\alpha - v_m),$$

wo α unbestimmt ist, ist dann eine symmetrische Function von $y_1, y_2 \dots y_m$ und kann deshalb rational ausgedrückt

werden. Die gesuchte Gruppe kann nur solche Substitutionen enthalten, welche den Werth von A unverändert lassen, dass heisst solche Substitutionen, welche die Grössen $v_1, v_2 \ldots v_m$ unverändert lassen oder unter einander vertauschen. Diese Substitutionen lösen also n Wurzeln desselben Systems

$$x_{\rho,1}, x_{\rho,2}, \ldots x_{\rho,n}$$

durch n Wurzeln desselben Systems ab; die Gruppe ist deshalb imprimitiv.

Andererseits sei die Gruppe G einer Gleichung imprimitiv und enthalte die m Systeme Buchstaben

$$x_{\rho,1}, x_{\rho,2} \ldots x_{\rho,n}$$

für

$$\rho = 1, 2, \ldots m.$$

Man setze

$$v_\rho = (\beta - x_{\rho,1})(\beta - x_{\rho,2}) \ldots (\beta - x_{\rho,n})$$

und

$$A = (\alpha - v_1)(\alpha - v_2) \ldots (\alpha - v_m),$$

wo α und β unbestimmt sind. A bleibt dann unverändert durch jede Substitution, welche Buchstaben desselben Systems durch Buchstaben desselben Systems ablöst. A bleibt also unverändert durch alle Substitutionen der Gruppe und kann deshalb rational ausgedrückt werden. Mit Hülfe von A können nun alle symmetrischen Functionen von $v_1, v_2 \ldots v_m$ rational ausgedrückt werden, so dass v mit den Werthen $v_1, v_2 \ldots v_m$ durch eine Gleichung m^{ten} Grades mit rationalen Coefficienten bestimmt wird; sobald v_ρ gefunden ist, wird x_ρ auf ähnliche Weise durch eine Gleichung n^{ten} Grades bestimmt, deren Coefficienten rationale Functionen von v_ρ sind.

Reduction der Gruppe durch adjungirte Grössen.

196. Die Ordnung von G ist der Grad der irreductiblen Gleichung in y; bewirkt nun die Adjungirung gewisser neuer Grössen, dass diese Gleichung sich zerlegen lässt, so erhält man eine neue Gruppe von niedrigerer Ordnung; da die Substitutionen dieser durch die Wurzeln bestimmt werden, welche der neuen irreductiblen Gleichung angehören, und diese Wurzeln unter den Wurzeln $y_1, y_2 \ldots y_m$ vorkommen, so muss die neue Gruppe in der ursprünglichen enthalten sein.

197. *Wenn man den Werth z_1 einer gewissen rationalen Function der Wurzeln adjungirt, so wird die reducirte Gruppe aus den Substitutionen von G bestehen müssen, durch welche der Zahlenwerth z_1 dieser Function unverändert bleibt.*

Da nämlich z_1 eine adjungirte Grösse ist, ist dieselbe als rational zu betrachten; jede Substitution der neuen Gruppe muss deshalb die gegebene Function der Wurzeln den Werth z_1 behalten lassen; auf der anderen Seite ist die neue Gruppe in der ursprünglichen mit enthalten; dieselbe kann deshalb nur aus solchen Substitutionen dieser Gruppe bestehen, welche den Werth der gegebenen Function nicht verändern.

Es muss noch bewiesen werden, dass alle Substitutionen von G, welche den Werth von z_1 nicht verändern, der reducirten Gruppe angehören; es möge deshalb eine beliebige Function der Wurzeln untersucht werden, welche rational durch z_1 und bekannte Grössen ausgedrückt werden kann; man hat dann, wenn U_1 diese Function und φ eine rationale Function bedeutet,

$$U_1 = \varphi(z_1),$$

woraus (193),

$$U_a = \varphi(z_a),$$

wo der Index a anzeigt, dass eine Substitution a ausgeführt wurde, welche eine beliebige von denjenigen Substitu-

tionen von G ist, die den Werth von z_1 nicht verändern; nun ist indessen

$$z_a = z_1, \text{ also } U_a = U_1,$$

so dass die Substitution a jede Function unverändert lässt, welche rational durch z_1 und früher benutzte Grössen ausgedrückt wird. a gehört also wirklich nach Adjungirung von z_1 zur Gruppe der Gleichung.

198. *Wenn eine Function φ der Wurzeln, ebenso wie eine andere Function π, durch dieselben G angehörigen Substitutionen unverändert bleibt, so kann φ rational durch π ausgedrückt werden.*

Adjungirt man nämlich π, so erhält die Gleichung eine reducirte Gruppe H; die Substitutionen dieser lassen π und deshalb auch φ unverändert; φ kann deshalb auch rational durch die adjungirte Grösse π und bekannte Grössen ausgedrückt werden.

Adjungirung der Wurzeln einer Hülfsgleichung.

199. Es sei z_1 eine Wurzel einer irreductiblen Hülfsgleichung mit den Wurzeln $z_1, z_2 \ldots z_k$; ferner wird angenommen, dass die Gruppe G reducirt wird, wenn man z_1 adjungirt. Die Gleichung $F(y) = 0$ theilt sich dann in mehrere irreductible Gleichungen desselben Grades, und jede von diesen bestimmt die reducirte Gruppe; eine von diesen Gleichungen sei

$$\varphi(y, z_1) = 0; \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

dieselbe kann so dargestellt werden, dass die höchste Potenz von y den Coefficienten 1 hat, während die übrigen Coefficienten ganze rationale Functionen von z_1 sind, deren höchster Exponent $k - 1$ nicht übersteigt.

Dividirt man $F(y)$ durch $\varphi(y, z_1)$ und setzt die Coefficienten des Restes gleich Null, so erhält man die Bedingungen dafür, dass $\varphi(y, z_1)$ in $F(y)$ aufgeht. Diesen Bedingungsgleichungen wird durch $z = z_1$ genügt, und da die Gleichung in z irreductibel ist, muss ihr also auch durch $z = z_2, \ldots z = z_k$ genügt werden. $F(y)$ ist also auch theilbar durch $\varphi(y, z_2) \ldots \varphi(y, z_k)$.

Das Product

$$\Psi(y) = \varphi(y, z_1)\,\varphi(y, z_2) \ldots \varphi(y, z_k) \quad \ldots\ldots\ldots (2)$$

ist eine symmetrische Function von y und bekannten Grössen (die Werthe von z sind hier nicht mit einbegriffen). Da jeder der Factoren ein Factor von $F(y)$ ist, kann die Gleichung

$$\Psi(y) = 0 \quad \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

keine anderen Wurzeln haben als $F(y) = 0$, und sie muss diese Wurzeln jede gleich oft haben, z. B. q mal; es muss dann identisch

$$\Psi(y) = [F(y)]^q \quad \ldots\ldots\ldots\ldots\ldots\ldots (4)$$

sein.

Da $\varphi(y, z_1) = 0$ irreductibel ist, muss jede der analogen Gleichungen es auch sein, wenn für jede derselben der darin vorkommenden Werth von z als adjungirt genommen wird. Wäre nämlich $\varphi(y, z)$ theilbar durch $\varphi_1(y, z)$ für $z = z_i$, so müsste der Rest, welchen φ bei der Division durch φ_1 lässt für $z = z_i$ Null werden; dann müsste er auch für $z = z_1$ Null werden, wodurch $\varphi(y, z_1) = 0$ reductibel würde; das würde aber den gemachten Voraussetzungen widerstreiten.

Falls zwei der Gleichungen $\varphi = 0$ eine Wurzel gemeinschaftlich haben, müssen sie alle Wurzeln gemeinschaftlich haben; angenommen

$$\varphi(y, z_1) = 0 \text{ und } \varphi(y, z_2) = 0 \quad \ldots\ldots\ldots\ldots (5)$$

hätten beide die Wurzel y_1, und die erste der beiden

Gleichungen habe ausserdem die Wurzel y_2. y_2 kann rational durch y_1 ausgedrückt werden, so dass

$$y_2 = \theta(y_1) \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (6)$$

wo θ eine rationale Function bedeutet. Die Gleichung

$$\varphi(\theta(y), z_1) = 0 \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (7)$$

hat dann eine Wurzel mit der ersten Gleichung (5) gemeinschaftlich und muss deshalb alle Wurzeln dieser Gleichung haben. Die Function

$$\varphi(\theta(y), z)$$

ist deshalb theilbar durch $\varphi(y, z)$ für $z = z_1$ und also auch für $z = z_2$, so dass die Gleichung

$$\varphi(\theta(y), z_2) = 0 \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (8)$$

von den Wurzeln der Gleichung $\varphi(y, z_2) = 0$ befriedigt werden muss; unter diesen Wurzeln befindet sich y_1, so dass man identisch

$$\varphi(\theta(y_1), z_2) = 0 \text{ oder } \varphi(y_2, z_2) = 0 \quad \ldots\ldots\ldots \quad (9)$$

hat, woraus hervorgeht, dass y_2 eine Wurzel der zweiten Gleichung (5) ist. Zwei von den Gleichungen $\varphi = 0$ haben also entweder dieselben oder lauter verschiedene Wurzeln.

Ist nun y_1 eine Wurzel von q dieser Gleichungen, so müssen diese alle dieselben Wurzeln haben; q andere Gleichungen müssen dann ein System von Wurzeln haben, unter denen keine der vorhergehenden vorkommt und so fort; durch Ausziehen der q^{ten} Wurzel aus (4) muss man also identisch erhalten

$$F(y) = \varphi(y, z_1)\,\varphi(y, z_2) \ldots \varphi(y, z_r), \quad \ldots\ldots\ldots \quad (10)$$

wo $\varphi(y, z_1) \ldots \varphi(y, z_r)$ einen von jedem System von identischen Factoren φ bedeuten, und wo deshalb $k = qr$.

Die Wurzeln z müssen sich also auf r Systeme mit q in jedem vertheilen, und zwar derartig, dass man zwei verschiedene reducirte Gruppen erhält, wenn man die eine oder

die andere von zwei Wurzeln, welche zu verschiedenen Systemen gehören, adjungirt, dagegen dieselbe reducirte Gruppe, wenn die beiden Wurzeln demselben Systeme angehören.

Falls der Grad k der Hülfsgleichung eine Primzahl p ist, muss $q = 1$ sein. F(y) erhält dann p Factoren, so dass man die Ordnung der reducirten Gruppe findet, wenn man die Ordnung von G durch p dividirt.

Adjungirt man eine gewisse Function der Wurzeln einer Gleichung, so adjungirt man in Wirklichkeit eine Wurzel der irreductiblen Gleichung, welche diese Function bestimmt. Die Werthe der Functionen bilden deshalb verschiedene Systeme auf die oben angegebene Weise.

200. *Die verschiedenen reducirten Gruppen sind ähnlich.* Zwei dieser Gruppen, z_1 und z_2 entsprechend, seien H_1 und H_2, und y_1 und y_2 seien beziehungsweise Wurzeln von

$$\varphi(y, z_1) = 0 \text{ und } \varphi(y, z_2) = 0.$$

Die Wurzeln der ersten dieser Gleichungen können dann durch

$$y_1, \theta_1(y_1), \theta_2(y_1) \ldots$$

ausgedrückt werden, wo θ_1, $\theta_2 \ldots$ gewisse rationale Functionen bedeuten; man kann dann leicht wie oben beweisen, dass die Wurzeln der zweiten Gleichung durch

$$y_2, \theta_1(y_2), \theta_2(y_2) \ldots$$

ausgedrückt werden können.

Nun sei T die Substitution, welche man ausführt, wenn man y_2 an Stelle von y_1 setzt, S_k und S'_k die Substitutionen, welche man ausführt, wenn man $\theta_k(y_1)$ an Stelle von y_1 und $\theta_k(y_2)$ an Stelle von y_2 setzt; dann hat man

$$T S_k = S'_k T,$$

da beide diese Substitutionen $\theta_k(y_2)$ an Stelle von y_1 setzen. Diese Gleichung zeigt, dass die Substitution S'_k der S_k ähn-

lich ist; S_k ist aber eine beliebige Substitution der Gruppe H_1, während S'_k eine Substitution der Gruppe H_2 ist. Die Substitution T transformirt also H_1 in H_2. Da y_1 und y_2 zwei beliebige Wurzeln von (3) sind, wird eine beliebige Substitution in G eine Gruppe H in dieselbe oder in eine andere Gruppe H transformiren.

201. *Falls die Wurzeln der irreductiblen Hülfsgleichung rational durch eine derselben ausgedrückt werden können und die Adjungirung einer derselben G auf H reducirt, muss H mit allen Substitutionen in G permutabel sein.*

Wenn alle Wurzeln der Hülfsgleichung rational durch eine derselben ausgedrückt werden können, so kann jede von ihnen rational durch eine beliebige der übrigen ausgedrückt werden; adjungirt man deshalb eine von ihnen, so ist das dasselbe, wie wenn man sie alle adjungirt; die verschiedenen Gruppen H_1, H_2, . . ., welche oben gefunden wurden, müssen deshalb übereinstimmen; da nun diese Gruppen durch alle Substitutionen der Gruppe G in einander transformirt wurden, muss H bei der Transformation durch alle diese Substitutionen unverändert bleiben. H ist also permutabel mit allen Substitutionen in G.

Dieser Fall tritt z. B. ein, wenn die Gruppe durch Adjungirung einer Wurzel der Gleichung $z^p = A$ reducirt wird, wenn A und die Wurzeln der Einheit als vorher adjungirt angenommen werden.

202. *Wenn die Adjungirung aller Wurzeln einer irreductiblen Hülfsgleichung G auf H reducirt, so ist H mit allen Substitutionen der Gruppe G permutabel.*

Die Adjungirung aller Wurzeln hat nämlich dieselbe Wirkung wie die Adjungirung einer Function φ der Wurzeln der Hülfsgleichung mit lauter verschiedenen Werthen; diese Werthe können rational durch einen derselben ausgedrückt werden, und die Wurzeln der Hülfsgleichung können rational durch φ ausgedrückt werden, so dass man alle Wurzeln der Gleichung in φ als adjungirt betrachten kann. Der Satz folgt dann aus 201.

203. *Falls G von der Ordnung $m = kq$ eine Gruppe H von der Ordnung q enthält, welche mit alle Substitutionen von G permutabel ist, wird G auf H reducirt werden, sobald die Wurzeln einer gewissen Abelschen Gleichung vom Grade k adjungirt werden.*

H bestehe aus den Substitutionen

$$1, S_1, S_2 \ldots S_{q-1};$$

alle Substitutionen von G können dann in k Reihen angeordnet werden; sie sind von der Form $T_\alpha S_\beta$, wo α für Substitutionen derselben Reihe denselben Werth hat.

Es seien $y_1, y_2 \ldots y_q$ die Wurzeln von $F(y) = 0$, welche aus y_1 durch die Substitutionen S gebildet werden, und es sei

$$\theta_1 = (\alpha - y_1)(\alpha - y_2) \ldots (\alpha - y_q),$$

wo α unbestimmt ist. θ_1 behält dann seinen Werth durch die Substitutionen S, wird aber durch alle übrigen Substitutionen verändert. Wenn θ_1 adjungirt wird, wird deshalb die Gruppe der Gleichung auf H reducirt.

Nun lässt sich zeigen, dass θ_1 durch eine Abelsche Gleichung vom Grade k bestimmt wird. Es mögen $\theta_1, \theta_2 \ldots \theta_k$ die Functionen sein, welche aus θ_1 durch die Substitutionen $1, T_1, \ldots T_{k-1}$ gebildet werden, und man setze

$$A = (\beta - \theta_1)(\beta - \theta_2) \ldots (\beta - \theta_k),$$

wo β unbestimmt ist.

Da H mit allen Substitutionen von G permutabel ist, wird keine der Functionen θ durch die Substitutionen S verändert werden (181). A kann dann nicht durch irgend welche Substitution $T_\beta S_\alpha$ verändert werden, denn S_α verändert kein θ, und T_β vertauscht nur die Functionen unter einander; man hat nämlich beispielsweise

$$T_\beta \cdot \theta_3 = T_\beta T_2 \theta_1 = T_\gamma S_\delta \cdot \theta_1 = \theta_{\gamma+1},$$

da $T_\beta T_2$ unter den Substitutionen von G vorkommen und deshalb die Form $T_\gamma S_\delta$ haben muss.

Da demnach keine der Substitutionen von G A verändert, kann A rational ausgedrückt werden. θ_1, θ_2 ... werden dann durch eine Gleichung vom k^{ten} Grade bestimmt und diese Gleichung, die leicht als irreductibel erkannt wird, ist eine Abelsche, denn die verschiedenen Werthe von θ können rational durch einander ausgedrückt werden, da sie durch dieselben Substitutionen von G unverändert bleiben. Ihre Gruppe ist von der Ordnung k und besteht aus den Substitutionen, welche θ_1, θ_2 ... auf dieselbe Weise wie die Substitutionen T versetzen.

Wenn k eine Primzahl ist, können die Wurzeln der Abelschen Gleichung rational durch die Wurzeln einer binomischen Gleichung ausgedrückt werden; man kann dann auch durch Adjungirung einer Wurzelgrösse und der Wurzeln der Einheit G auf H reduciren.

204. Nunmehr kann man die nothwendigen und ausreichenden Bedingungen dafür angeben, dass eine Gleichung algebraisch aufgelöst werden kann. Kann die Gleichung algebraisch aufgelöst werden, so muss ihre Gruppe auf 1 reducirt werden, sobald man nach und nach alle bei der Auflösung vorkommenden Wurzelgrössen und Wurzeln der Einheit adjungirt, da dadurch alle Wurzeln der Gleichung in y bekannt werden. Die Gruppe muss also auf 1 reducirt werden, wenn man nach und nach die Wurzeln gewisser Hülfsgleichungen von der Form

$$z^p = A$$

adjungirt, wo p eine Primzahl und A eine bekannte oder früher adjungirte Grösse bedeutet; diese Gleichung ist eine Abelsche, wenn die Wurzeln der Einheit als bekannt angenommen werden.

Indessen wurde in 199 und 203 bewiesen, dass die nothwendige und ausreichende Bedingung dafür, dass die Gruppe

G der Gleichung, von der Ordnung pq, durch eine solche Adjungirung reducirt werde, darin besteht, dass sie eine Gruppe H von der Ordnung q enthält, welche mit allen Substitutionen von G permutabel ist. H muss dann eine neue Gruppe enthalten, welche mit allen Substitutionen von H permutabel ist u. s. w., bis man zur Gruppe 1 gelangt; also:

Die nothwendige und ausreichende Bedingung dafür, dass eine Gleichung algebraisch aufgelöst werden könne, besteht darin, dass ihre Gruppe eine andere Gruppe enthält, diese wieder eine andere u. s. w., bis man zur Gruppe 1 gelangt, und zwar muss diese Reihe von Gruppen so beschaffen sein, dass jede von ihnen mit allen Substitutionen der vorhergehenden permutabel ist, und dass ihre Ordnung aus der Ordnung der vorhergehenden durch Division mit einer Primzahl gefunden wird.

205. Als Beispiel möge die allgemeine Gleichung vierten Grades dienen; die Gruppe derselben ist die vollständige Gruppe vom 4ten Grade und von der 24sten Ordnung; dieselbe enthält die alterne Gruppe, mit welcher alle ihre Substitutionen permutabel sind; sie wird deshalb durch Adjungirung einer alternirenden Function der Wurzeln auf die alterne Gruppe reducirt; es ist dieselbe, welche man bei dem ersten Ausziehen der Quadratwurzel, welches bei der Auflösung der Gleichung ausgeführt wird, findet.

Die alterne Gruppe enthält eine Gruppe von der 4ten Ordnung, welche mit allen Substitutionen der alternen Gruppe permutabel ist, nämlich

$$1, \ (x_1 x_2)(x_3 x_4), \ (x_1 x_3)(x_2 x_4), \ (x_1 x_4)(x_2 x_3);$$

durch Ausziehen einer Kubikwurzel wird eine Function bestimmt, welche durch diese Substitutionen nicht verändert wird, z. B. $x_1 x_2 + x_3 x_4$; wird diese adjungirt, so wird die alterne Gruppe auf die angeführte von der 4ten Ordnung reducirt, welche wiederum durch zweimaliges Ausziehen der Quadratwurzel auf die Gruppe 1 reducirt wird.

Die vollständige Gruppe n^{ten} Grades, welche der allgemeinen Gleichung n^{ten} Grades angehört, kann durch Ausziehen einer Quadratwurzel auf die alterne Gruppe reducirt werden; es lässt sich zeigen, dass diese Gruppe für $n > 4$ einfach ist, und dieselbe kann daher für solche Werthe von n durch Adjungirung von Wurzelgrössen nicht weiter reducirt werden; hieraus folgt dann, dass die allgemeine Gleichung von höherem als dem vierten Grade nicht algebraisch aufgelöst werden kann.

Der erwähnte Beweis lässt sich so führen: Man nehme an, dass die alterne Gruppe G von der Ordnung $\frac{1}{2}n!$ sich auf eine Gruppe K von der Ordnung k reduciren liesse, wo $kp = \frac{1}{2}n!$, und wo p eine Primzahl ist. K kann nicht alle cyclischen Substitutionen dritter Ordnung enthalten. Man kann dann eine neue Gruppe von der Ordnung $3k$ bilden (161), welche in G einbegriffen ist. Man muss also $p = 3$ haben. Ist $n > 4$, erhält man auf die nämliche Weise $p = 5$, indem K nicht alle cyclischen Substitutionen fünfter Ordnung enthalten kann. Die Reduction ist also unmöglich für $n > 4$.

Dieser Beweis ist in der That der nämliche, der früher geführt wurde, um die Unmöglichkeit der algebraischen Auflösung der Gleichung fünften Grades darzuthun.

Viertes Kapitel.

Anwendungen der Theorie von Galois.

Abelsche Gleichungen.

206. Die Abelschen Gleichungen sind schon im Vorhergehenden ausführlich behandelt worden; deshalb soll hier nur in Kürze gezeigt werden, wie die Theorie von Galois bei ihrer Behandlung angewendet werden kann.

In der irreductiblen Gleichung vom n^{ten} Grade ist

$$x_2 = \theta(x_1) \text{ oder } x_2 - \theta(x_1) = 0; \quad \ldots \ldots \ldots \quad (1)$$

die Gruppe der Gleichung muss eine Substitution enthalten, welche x_2 an Stelle von x_1 setzt; ein Cyclus aus dieser sei

$$(x_1 x_2 x_3 \ldots x_r);$$

diese Substitution kann auf (1) angewendet werden, wodurch man

$$\theta(x_1) = x_2; \ \theta(x_2) = x_3; \ \ldots \theta(x_r) = x_1 \quad \ldots \ldots \quad (2)$$

erhält.

Man sieht nun leicht, dass eine Substitution der Gruppe, welche einen von den Buchstaben $x_1, x_2 \ldots x_r$ durch einen Buchstaben ablöst, welcher unter diesen nicht vorkommt, sie

alle durch neue Buchstaben ablösen muss, da die Gleichung im entgegengesetzten Fall gleiche Wurzeln haben müsste; wird die erste Substitution durch die letzte transformirt, so erhält man eine Substitution, welche zeigt, dass r von der ersten verschiedene Wurzeln durch Gleichungen verbunden sind, die den Gleichungen (2) analog sind; sind mehr Wurzeln vorhanden, müssen auch diese in Systeme von je r Wurzeln zerfallen, und die Substitutionen der Gruppen können nur Wurzeln desselben Systems durch Wurzeln desselben Systems ablösen. Die Gruppe ist deshalb imprimitiv, und die Gleichung kann durch eine Hülfsgleichung in Gleichungen vom Grade r zerlegt werden, welche die einzelnen Systeme von Wurzeln bestimmen.

207. Man hat also nur nöthig solche Gleichungen zu betrachten, deren Gruppen eine cyclische Substitution von allen Wurzeln enthalten, und wo $x_2 = \theta(x_1)$. Alle Wurzeln können dann rational durch eine derselben ausgedrückt werden, und jede Function der Wurzeln erhält nur n Werthe. Die Gleichung $F(y) = 0$, welche die Gruppe bestimmt, ist deshalb höchstens vom n^{ten} Grade, und sie muss dann genau vom n^{ten} Grade sein, da die Gruppe transitiv ist und ihre Ordnung deshalb theilbar ist durch n. Die Gruppe wird dann von einer cyclischen Substitution $(x_1 x_2 \ldots x_n)$ und deren Potenzen gebildet.

Ist nun $\alpha^n = 1$ (α eine primitive Wurzel), so sieht man leicht, dass die Grösse

$$A = (\alpha x_1 + \alpha^2 x_2 + \ldots x_n)^n$$

rational ist, da der Werth derselben nicht durch die Substitutionen der Gruppe verändert wird; wird $\sqrt[n]{A}$ und α adjungirt, so wird die Gruppe auf 1 reducirt, da alle übrigen Substitutionen $\alpha x_1 + \alpha^2 x_2 + \ldots x_n$ verändern; die Wurzeln der Gleichung werden deshalb rational durch $\sqrt[n]{A}$ und die Wurzeln der Einheit ausgedrückt.

Ist der Grad einer Abelschen Gleichung eine Primzahl n, so muss die Gruppe eine cyclische Substitution von der Ordnung n enthalten; die Gleichung kann dann immer algebraisch aufgelöst werden. Ist n keine Primzahl, während die Gruppe dennoch eine cyclische Substitution von der n^{ten} Ordnung enthält, so sieht man leicht, dass man nach und nach die Gruppe dadurch reduciren kann, dass man Wurzelgrössen, deren Exponenten Primzahlen sind, adjungirt; ist z. B. $n = 15$ und S die cyclische Substisution, so bilden

$$1, S^3, S^6, S^9, S^{12}$$

eine Gruppe, welche mit alle Substitutionen der ursprünglichen Gruppe permutabel ist, und welche die reducirte Grüppe wird, wenn man die Wurzeln einer Gleichung von der Form

$$z^3 = A$$

adjungirt.

Die Galoissche Gleichung.

208. Galois hat irreductible Gleichungen betrachtet, deren Grad p eine Primzahl ist, und deren Wurzeln alle rational durch zwei derselben ausgedrückt werden können, und derselbe hat gezeigt, dass solche Gleichungen algebraisch aufgelöst werden können.

Da jede rationale Function der Wurzeln rational durch die beiden Wurzeln ausgedrückt werden kann, kann die Ordnung der Gruppe höchstens $p(p-1)$ sein; da die Gruppe transitiv ist, ist die Ordnung derselben theilbar durch p.

Es wurde früher (186) gezeigt, dass die Substitutionen einer solchen Gruppe, wenn die Wurzeln $x_0, x_1, \ldots x_{p-1}$ sind, alle von der Form

$$\binom{az+b}{z}$$

oder von der Form

$$T^{\alpha} S^{\beta}$$

sind, wo

$$S = \binom{z+1}{z};\ T = \binom{az}{z}.$$

Die Ordnung der Gruppe ist kp, wo k gleich $p-1$ oder ein Divisor von $p-1$ ist, und a ist eine primitive Wurzel von

$$a^k \equiv 1 \text{ (mod. p)}.$$

Nun setze man

$$X_1 = (x_0 + \alpha x_1 + \alpha^2 x_2 + \ldots + \alpha^{p-1} x_{p-1})^p,$$

wo α eine Wurzel von $\frac{x^p - 1}{x - 1} = 0$ ist. Aus X_1 bilde man nun durch $T, T^2 \ldots T^{k-1}$ die analogen Ausdrücke X_2, $X_3 \ldots X_k$; setzt man dann

$$A = (X_1 + \beta X_2 + \beta^2 X_3 \ldots + \beta^{k-1} X_k)^k,$$

wo β eine beliebige Wurzel der Gleichung $x^k - 1 = 0$ ist, so muss A rational sein. A wird nämlich nicht durch die Substitutionen der Gruppe verändert, denn die Substitution S verändert nicht X_1, $X_2 \ldots$, und die Substitution T bewirkt eine cyclische Verschiebung von X_1, $X_2 \ldots$.

Ertheilt man nun β nach und nach seine verschiedenen Werthe, so erhält man k Gleichungen ersten Grades aus denen X_1, $X_2 \ldots$ gefunden werden, rational durch die Wurzeln der Einheit und durch die Grösse

$$\sqrt[k]{A}$$

ausgedrückt.

Aus X_1, $X_2 \ldots$ findet man wiederum x_0, $x_1 \ldots$, wie es bei der Behandlung von Abelschen Gleichungen gezeigt wurde. In Wirklichkeit wird die gegebene Gleichung auf eine Abelsche Gleichung durch Adjungirung einer dieser Grössen redu-

cirt, da die Gruppe dadurch auf Potenzen von S reducirt wird. Folglich:

Eine irreductible Gleichung, deren Grad eine Primzahl ist, und deren Wurzeln alle rational durch zwei derselben ausgedrückt werden können, lässt sich algebraisch auflösen.

Falls die Gruppe, welche einer irreductiblen Gleichung vom Grade p angehört, nur lineare Substitutionen enthält, kann andererseits jede der Wurzeln durch zwei beliebige derselben ausgedrückt werden; denn adjungirt man zwei der Wurzeln, so wird die Gruppe auf 1 reducirt, da alle linearen Substitutionen, 1 ausgenommen, wenigstens $p-1$ Wurzeln versetzen und deshalb nicht zwei derselben unverändert lassen können.

209. *Falls eine irreductible Gleichung vom Grade p sich algebraisch auflösen lässt, kann die Gruppe derselben nur lineare Substitutionen enthalten.*

Adjungirt man die verschiedenen Wurzelgrössen um die Gruppe der Gleichung zu reduciren, so muss sich unter diesen eine p^{te} Wurzel finden, da man nur dadurch aus der Ordnung der Gruppe den Factor p entfernen kann. Sobald man diese Wurzel adjungirt, und nicht früher, wird die gegebene Gleichung reductibel; wird die Gleichung reductibel, so kann, weil die Gruppe intransitiv ist, die Ordnung der Gruppe nicht theilbar sein durch p, und andererseits kann die Gleichung nicht irreductibel sein, wenn aus der Ordnung der Gruppe der Factor p entfernt ist.

Die gegebene Gleichung ist also reductibel, nachdem die p^{te} Wurzel adjungirt worden ist, und ihre Gruppe ist deshalb intransitiv, falls sie nicht auf 1 reducirt ist. Diese intransitive Gruppe sei

$$H=(1, U_1, U_2 \ldots);$$

vor der Adjungirung bestand dann die Gruppe aus allen Substitutionen von der Form

$$S^\alpha U_\beta,$$

wo S eine cyclische Substitution von der p^{ten} Ordnung bedeutet (161).

Die Buchstaben zerfallen in mehrere Systeme, derartig dass die Substitutionen U nur Buchstaben desselben Systems unter einander vertauschen; H ist indessen permutabel mit den Potenzen von S; diese müssen deshalb nur Buchstaben desselben Systems durch Buchstaben desselben Systems ablösen können; da das mit den Potenzen von S nicht der Fall ist, kann H nur aus der Substitution 1 bestehen. Zuletzt muss also eine p^{te} Wurzel adjungirt worden sein, und vor dieser Adjungirung bestand die Gruppe aus den Potenzen einer cyclischen Substitution.

Da die Gruppe durch die letzte Adjungirung auf 1 reducirt wird, werden dadurch alle Wurzeln der gegebenen Gleichung rational, so dass die Gleichung, welche bis dahin irreductibel blieb, nunmehr in lauter Gleichungen ersten Grades zerfällt.

210. Die successiven Adjungirungen hätten die ursprüngliche Gruppe reduciren können, ohne doch $f(x) = 0$ reductibel zu machen. Falls eine solche Adjungirung eine Gruppe G auf eine Gruppe H reducirt hat, welche nur lineare Substitutionen enthält, so kann man beweisen, dass auch G nur lineare Substitutionen enthalten kann; dadurch wird dann der obenstehende Satz bewiesen sein, denn da die letzte Gruppe nur lineare Substitutionen enthält, muss dasselbe von allen früheren gelten.

Es muss also bewiesen werden, dass G nur lineare Substitutionen enthalten kann, falls H, welches aus G durch Adjungirung der Wurzeln einer binomischen Gleichung gebildet ist, nur lineare Substitutionen enthält. H muss die cyclische Substitution S von der p^{ten} Ordnung und deren Potenzen enthalten; T sei eine Substitution von G, welche nicht in H vorkommt. H ist permutabel mit T, und T muss deshalb S in eine Potenz von S transformiren, denn in der linearen Gruppe H kommen keine andere Substitutionen

vor, welche S ähnlich sind; als die Potenzen von S. T ist dann selber eine lineare Substitution, denn nur solche transformiren S in eine Potenz von S.

Dergestalt ist bewiesen, dass die von Galois angegebene Bedingung für die Möglichkeit der algebraischen Auflösung einer irreductiblen Gleichung, deren Grad eine Primzahl ist, sowohl ausreichend als auch nothwendig ist.

Gleichungen, bei denen die Ordnung der Gruppe eine Potenz einer Primzahl ist.

211. Die irreductible Gleichung $f(x) = 0$ möge eine Gruppe G haben, deren Ordnung p^n ist, wo p eine Primzahl bedeutet. Da die Ordnung durch den Grad der Gleichung theilbar ist, muss der Grad auch eine Potenz von p sein, z. B. p^m.

Adjungirt man eine Wurzel der Gleichung, x_1, so wird die Gleichung reductibel; jede der irreductiblen Gleichungen, in welche sie zerfällt, hat in ihrer Gruppe nur Substitutionen, deren Ordnung eine Potenz von p ist (194), so dass die Ordnung der Gruppe und folglich auch der Grad der Gleichung Potenzen von p sein müssen.

Da die Gleichung also durch Adjungirung von x_1 in irreductible Gleichungen zerlegt wird, deren Grade Potenzen von p sind, und unter diesen eine vom Grade 1 vorkommt, so müssen wenigstens p vom Grade 1 vorhanden sein; wenigstens p von den Wurzeln können also rational durch x_1 ausgedrückt werden. Oben (206) wurde gezeigt, dass die Gruppe solcher Gleichungen imprimitiv ist, und dass dieselben durch eine Hülfsgleichung reducirt werden können. Die Gruppe der reducirten Gleichung besteht aus Substitutionen, deren Cyclen unter den Substitutionen von G vorkommen, und die

Ordnung derselben, ebenso wie der Grad der Gleichung, sind deshalb Potenzen von p. Dividirt man mit dem Grade dieser Gleichung in den Grad der gegebenen Gleichung, so erhält man den Grad der Hülfsgleichung (195), der also auch eine Potenz von p ist. Die Ordnung der Gruppe der Hülfsgleichung muss auch eine Potenz von p sein, denn diese Gruppe wird auf 1 reducirt, wenn man alle Wurzeln der gegebenen Gleichung adjungirt; adjungirt man diese Wurzeln, eine zur Zeit, und erwägt man, dass man bei jeder neuen Zerlegung der gegebenen Gleichung zu irreductiblen Gleichungen gelangen muss, deren Ordnung und Grad Potenzen von p sind, so sieht man, dass die Ordnung der Gruppe der Hülfsgleichung eine Potenz von p sein muss (199). Zu demselben Resultat gelangt man, wenn man nachweist, dass diese Gruppe isomorph mit G ist.

Die beiden neuen Gleichungen können nun auf dieselbe Weise reducirt werden, bis man zu einem System Abelscher Gleichungen vom Grade p gelangt. Da das Product der Grade dieser Gleichungen gleich dem Grade der gegebenen Gleichung ist, kann also jede Wurzel von dieser mit Hülfe von m Abelschen Gleichungen p^{ten} Grades gefunden werden.

212. Andererseits wird die Ordnung der Gruppe einer Gleichung, welche mit Hülfe von lauter Abelschen Gleichungen p^{ten} Grades gelöst werden kann, nach und nach mittelst lauter Divisionen durch p auf 1 reducirt werden. Die Ordnung muss deshalb eine Potenz von p sein. Folglich:

Die nothwendige und ausreichende Bedingung dafür, dass eine Gleichung mit Hülfe von Abelschen Gleichungen p^{ten} Grades aufgelöst werden kann, besteht darin, dass die Ordnung ihrer Gruppe eine Potenz von p ist. Ihr Grad ist dann auch eine Potenz von p.

Man sieht, dass dieser Satz eine Erweiterung des Satzes ist, welcher früher über Gleichungen, welche durch Quadratwurzeln aufgelöst werden können, bewiesen wurde.

Der obenstehende Beweis zeigt, dass keine anderen transitiven Gruppen von der Ordnung p^n $(n > 1)$ existiren, als imprimitive. Der Beweis setzt freilich voraus, dass es eine Gleichung giebt, welche die gegebene Gruppe hat. Indessen entspricht jeder Gruppe eine Gleichung, nämlich die allgemeine Gleichung vom Grade der Gruppe, wenn man dieser eine Function der Wurzeln, die durch die Substitutionen der Gruppe und nicht durch andere Substitutionen unverändert bleibt, adjungirt denkt.

213. Eine Gruppe G möge eine Gruppe H von der Ordnung p^α enthalten, wo p eine Primzahl ist. Alle diejenigen Substitutionen von G, welche mit H permutabel sind, bilden eine Gruppe K von einer Ordnung $\mu\, p^\alpha$.

Angenommen es sei

$$H = (1, S_1, S_2 \ldots);$$

die Substitutionen von K können dann in Reihen von der Form

$$T_\gamma, T_\gamma S_1, \ldots$$

angeordnet werden.

Falls H diejenige von G's Untergruppen ist, für welche α so gross wie möglich ist, kann unter den Substitutionen $T_\gamma S_\beta$ keine vorkommen, deren Ordnung eine Potenz von p ist; denn wäre eine solche vorhanden, so könnte man mit Hülfe derselben aus H eine neue Gruppe von einer Ordnung p^β bilden, wo $\beta > \alpha$ (161). Da jede Substitution S eine Ordnung hat, welche eine Potenz von p ist, kann sie nicht einer der Substitutionen TS ähnlich sein.

Die Substitutionen von G können in Reihen angeordnet werden:

$$\begin{array}{l} 1\, S_1\, S_2 \ldots T,\; T S_1 \ldots \\ U\; US_1\, US_2 \ldots UT, \ldots \\ \ldots\ldots\ldots\ldots\ldots \end{array}$$

U ist nicht permutabel mit H, aber möglicherweise mit einer in H enthaltenen Gruppe, 1, S_α, $S_\beta \ldots$; die Substitutionen S können dann in Reihen wie

$$\begin{array}{l} 1,\ S_\alpha,\ S_\beta \ldots \\ M_1,\ M_1 S_\alpha,\ M_2 S_\beta \ldots \\ M_2,\ M_2 S_\alpha,\ M_2 S_\beta \ldots \\ \ldots\ldots\ldots\ldots \end{array}$$

geschrieben werden, worin die Anzahl der Substitutionen M eine Potenz von p ist.

Multiplicirt man die Reihe

$$U,\ US_1,\ US_2 \ldots$$

links mit einer der Substitutionen S_α, $S_\beta \ldots$, so erhält man wieder dieselbe Reihe, nur auf andere Weise geordnet, während die Multiplication mit einer der Substitutionen M die Reihe in eine neue Reihe übergehen lässt, welche lauter neue und unter einander verschiedene Substitutionen enthält; auf die Weise bildet man aus dieser Reihe so viele Reihen, wie es Substitutionen M giebt; die Anzahl dieser Reihen ist eine Potenz von p.

Enthält G mehr Substitutionen, bildet man aus einer von diesen auf ähnliche Weise Reihen, deren Anzahl eine Potenz von p ist, und so fährt man fort, bis alle Substitutionen von G berücksichtigt sind. Alle auf solche Weise gebildeten Substitutionen sind unter einander verschieden; die Ordnung von G ist deshalb

$$\mu p^\alpha (1 + p^{\alpha - \alpha_1} + p^{\alpha - \alpha_2} + \ldots),$$

wo p^{α_1}, $p^{\alpha_2} \ldots$ die Ordnungen der in H enthaltenen Gruppen bedeuten, mit welchen die Substitutionen der verschiedenen in G enthaltenen Systeme permutabel sind. Mehrere der Zahlen α_1, $\alpha_2 \ldots$ können gleich gross sein; auch können sie

Null sein und höchstens $\alpha - 1$. Der Ausdruck in der Klammer hat also jedenfalls die Form $1 + np$.

214. Nun soll die Gruppe K genauer untersucht und nachgewiesen werden, dass μ durch p nicht theilbar sein kann. Da H mit allen Substitutionen von K permutabel ist, kann man, wenn man eine Gleichung betrachtet, deren Gruppe K ist, K auf H durch eine Hülfsgleichung vom Grade μ, deren Wurzeln alle rational durch eine derselben ausgedrückt werden können, und deren Gruppe deshalb von der Ordnung μ ist, reduciren (203). Diese Gruppe muss eine Substitution von der Ordnung p enthalten, sobald μ durch p theilbar ist. Diese Substitution unter den Grössen, welche in 203 mit $\theta_1, \theta_2 \ldots$ bezeichnet wurden, kann dnrch eine der Substitutionen T ersetzt werden, und die p^{te} Potenz von dieser muss dann $\theta_1, \theta_2 \ldots$ unverändert lassen; da dies nur für die Substitutionen S gilt, muss T sich unter diesen finden, aber das würde mit sich führen, das die Ordnung von T eine Potenz von p wäre, was den gemachten Voraussetzungen widerspricht. μ ist deshalb nicht durch p theilbar.

Man sieht also, dass eine Gruppe, deren Ordnung kp^α, wo k nicht theilbar ist durch p, eine imprimitive Untergruppe von der Ordnung p^α oder eine lineare Gruppe p^{ter} Ordnnng, wenn $\alpha = 1$, enthalten muss. Die Gruppe von der Ordnung p^α ist mit enthalten in einer anderen von der Ordnung μp^α, mit deren Substitutionen sie permutabel ist, und man hat dann

$$k = \mu(np + 1).$$

215. Ist $k < p$, so muss $k = \mu$ sein; ist nun $\mu = \mu_1 p_1{}^\beta$, wo p_1 eine neue Primzahl bedeutet, welche nicht in μ_1 aufgeht, und ist $\mu_1 < p_1$, so kann die Hülfsgleichung vom Grade μ wieder durch eine Gleichung vom Grade μ_1 auf eine Gleichung reducirt werden, welche durch Wurzelgrössen aufgelöst werden kann; kann man auf diese Weise fortfahren, bis man zu einer Hülfsgleichung gelangt, deren Grad und

Ordnung eine Potenz einer Primzahl ist, so kann die gegebene Gleichung algebraisch aufgelöst werden. (Sylow, Math. Annalen V.)

Die Hessesche Gleichung.

216. Hesse hat eine Gleichung 9ten Grades untersucht von der Eigenschaft, dass zwei beliebige ihrer Wurzeln, a und b, mit einer dritten Wurzel c durch die Relationen

$$c = \varphi(a, b),\ b = \varphi(a, c),\ a = \varphi(b, c)$$

verbunden sind, wo φ eine rationale symmetrische Function bedeutet.

Zu einer solchen Gleichung gelangt man, wenn man die 9 Inflexionspunkte zu bestimmen sucht, welche eine Curve dritter Ordnung hat; für diese 9 Punkte gilt nämlich der Satz, dass eine durch zwei beliebige derselben gelegte Gerade noch durch einen dritten Punkt geht. Die Bedingung dafür, dass drei von den Punkten auf einer Geraden liegen, nimmt nun eben die Form $c = \varphi(a, b)$ an, wo a, b und c Wurzeln der Gleichung 9ten Grades sind, welche die Punkte bestimmt. Diese Bedingungsgleichung wird also nur befriedigt, wenn a, b und c drei solche Punkte sind, welche auf einer Geraden liegen.

217. Die Gruppe der Gleichung kann nun nur solche Substitutionen enthalten, welche a, b und c mit drei Punkten vertauschen, welche auch in gerader Linie liegen (193).

Zwei Punkte können aus 9 auf 72 verschiedene Arten mitnommen werden; auf die Weise zählt man indessen jede Linie 6 mal mit, so dass in Wirklichkeit 12 verschiedene gerade Linien vorhanden sind; zu demselben Resultat gelangt man, wenn man beachtet, dass von jedem Punkte 4 gerade Linien auslaufen, wodurch die Anzahl der Linien $4 . 9 : 3 = 12$ wird.

Von drei Punkten, welche auf einer Geraden liegen, laufen also ausser dieser 9 gerade Linien aus; die übrigen 6 Punkte müssen dann drei und drei auf den beiden fehlenden Linien liegen.

Nun bezeichne man jeden Punkt durch zwei Indices, und der erste von diesen sei 0, 1 oder 2, je nachdem der Punkt auf der ersten, zweiten oder dritten von diesen Linien liegt; von den übrigen 9 Linien wähle man drei auf dieselbe Weise und lasse den zweiten Index des Punktes, auf ähnliche Weise wie den ersten, diejenige von diesen Linien angeben, auf welcher der Punkt liegt.

Auf die Weise werden die Punkte durch

(00) (01) (02)
(10) (11) (12)
(20) (21) (22)

bezeichnet, während die 6 Linien diejenigen sind, welche die Punkte enthalten, welche in derselben Zeile oder in derselben Colonne stehn.

Man kann die Punkte nicht so anordnen, dass man auch die übrigen 6 Linien sieht, denn nur drei von den Punkten können reell sein. Die zwei fehlenden Linien, welche den Punkt (00) enhalten, können indessen nur

(00) (11) (22)

oder

(00) (12) (21)

sein

Die übrigen Linien werden auf dieselbe Weise bestimmt, und man sieht dann, dass die Punkte auf einer geraden Linie liegen, für welche sowohl die Summe der ersten als auch der zweiten Indices theilbar ist durch 3.

218. Bezeichnet man nun die beiden Indices durch x und y und bildet Substitutionen, welche x und y beziehungs-

weise durch $ax + by + c$ und $a_1 x + b_1 y + c_1$ ablösen, wo die Zahlen nach dem Modulus 3 zu nehmen sind, so werden diese immer an Stelle von drei in gerader Linie liegenden Punkte wiederum drei in gerader Linie liegende Punkte setzen, da

$$x_1 + x_2 + x_3 \equiv y_1 + y_2 + y_3 \equiv 0$$

zur Folge hat, dass

$$ax_1 + by_1 + c + ax_2 + by_2 + c + ax_3 + by_3 + c \equiv 0.$$

Durch

$$(x, y;\ ax + by + c,\ a_1 x + b_1 y + c_1)$$

wird eine Substitution der 9 Punkte repräsentirt, sobald man nur die Werthe von a, b, a_1 und b_1 ausschliesst, für welche $ab_1 - ba_1 \equiv 0$. Diese Substitutionen bilden eine Gruppe, da das Product von zweien wieder eine derselben giebt. c und und c_1 können 0, 1 und 2 sein; sind c und c_1 gewählt, so können a und b alle ihre Werthe erhalten mit Ausnahme von 0 und 0; sind a und b gewählt, so kann man man a_1 und b_1 auf 6 Arten wählen; die Ordnung der Gruppe ist also 9 . 8 . 6.

Die hier gefundene Gruppe G löst drei in gerader Linie liegende Punkte durch drei in gerader Linie liegende Punkte ab; es lässt sich zeigen, dass sie alle Substitutionen enthält, welche diese Eigenschaft besitzen.

T sei eine solche Substitution, welche (00) durch $(\alpha\beta)$, (01) durch $(\alpha_1 \beta_1)$ ablöst; dieselbe muss dann (02) durch einen solchen Punkt $(\alpha_2 \beta_2)$ ablösen, dass

$$\alpha + \alpha_1 + \alpha_2 \equiv \beta + \beta_1 + \beta_2 \equiv 0.$$

In der Gruppe G werden die Substitutionen

$$S = (x, y;\ ax + by + \alpha,\ a_1 x + b_1 y + \beta),$$

wo

$$b + \alpha \equiv \alpha_1;\ b_1 + \beta \equiv \beta_1,$$

die drei Punkte gerade auf dieselbe Weise ablösen.

T möge ferner (10) durch $(\alpha_3\, \beta_3)$ ablösen; dasselbe wird dann von S gelten, wenn a und a_1 so gewählt werden, dass

$$a + \alpha \equiv \alpha_3,\ a_1 + \beta \equiv \beta_3.$$

Man sieht leicht, dass die Substitution T nun vollkommen bestimmt ist, und zwar allein durch die Bedingung, dass drei in gerader Linie liegende Punkte durch drei in gerader Linie liegende Punkte abgelöst werden; da die Substitution S, welche bestimmt wurde, diese Bedingung erfüllt, so stimmt sie mit T überein.

G enthält also alle diejenigen Substitutionen, welche den Werth Null von $\varphi(a, b) - c$ nicht verändern. G ist deshalb die Gruppe der Gleichung oder enthält jedenfalls die Gruppe der Gleichung.

219. G enthält die Gruppe G_1, mit den Substitutionen

$$(x, y;\ ax + c,\ ay + c_1),$$

wo a 1 oder 2 ist, während c und c_1 alle ihre Werthe haben. Diese Gruppe von der 18ten Ordnung ist mit allen Substitutionen von G permutabel. Sucht man drei Linien, welche alle 9 Punkte enthalten, so sieht man leicht, dass G_1 eben die Substitutionen von G enthält, welche diese Linien nur unter einander vertauschen. Da 12 Linien vorhanden sind, kann man 4 solche Systeme von Linien bilden; diese 4 Systeme müssen deshalb durch eine Gleichung 4ten Grades bestimmt werden; durch Auflösung dieser wird die Gruppe auf G_1 reducirt.

Die Gruppe wird auch auf G_1 reducirt, wenn man eine Abelsche Gleichung vom Grade $9 . 8 . 6 : 18 = 24$ auflöst; diese Gleichung ist indessen nichts anderes als die Resolvente einer Gleichung vierten Grades und ist deshalb aufgelöst,

sobald diese gelöst ist. Anstatt die Gruppe G sofort auf G_1 zu reduciren, hätte man sie nach und nach reduciren können, indem man die Wurzelgrössen adjungirt, welche bei der Auflösung der Gleichung vierten Grades eingeführt werden; dadurch würde eben die Ordnung von G durch 24 dividirt werden.

G_1 enthält die Gruppe G_2 von der dritten Ordnung

$$(x, y; x, y + c_1),$$

welche mit allen Substitutionen von G_1 permutabel ist; die Gruppe der Gleichung wird also auf G_2 reducirt, wenn man eine Gleichung dritten Grades, welche die drei Linien des Systemes bestimmt, auflöst, oder wenn man die Wurzelgrössen adjungirt, welche bei der Auflösung dieser Gleichung eingeführt werden.

Die Gruppe ist nun auf die Potenzen einer regelmässigen Substitution der dritten Ordnung reducirt; dieselbe ist also intransitiv, und die Gleichung ist deshalb nun in drei Gleichungen dritten Grades zerlegt; diese Gleichungen sind Abelsche Gleichungen, da die Gruppe auf 1 reducirt wird, sobald man eine beliebige von den Wurzeln adjungirt.

Monodromiegruppe einer Gleichung.

220. Es sei

$$f(x, k) = 0$$

eine Gleichung, in deren Coefficienten ein unbestimmter Parameter k vorkommt, während im Uebrigen der Einfachheit wegen angenommen werden möge, dass die Coefficienten numerisch seien. Wird k als bekannt betrachtet, so hat die Gleichung eine gewisse Gruppe G.

Eine rationale Function φ von k und den Wurzeln, welche nicht durch die Substitutionen von G verändert wird,

kann rational durch k und bekannte Zahlen ausgedrückt werden. Dieselbe muss deshalb eine *monodrome* Function von k sein, das heisst, sie muss, wenn sie für einen gewissen Werth von k einen gewissen Werth hat, wiederum denselben Werth erhalten, sobald k, nachdem es sich auf eine beliebige Weise continuirlich verändert hat, wiederum seinen ursprünglichen Werth annimmt. Die Function erhält nach dieser Veränderungen wiederum ihren ursprünglichen numerischen Werth, aber die algebraische Form derselben wird in der Regel eine andere sein, da die Aenderung von k eine gewisse Vertauschung unter den Wurzeln mit sich bringen wird.

Lässt man k sich reell und imaginär auf alle möglichen Arten ändern, so werden, wie angeführt, gewisse Substitutionen unter den Wurzeln ausgeführt. Diese Substitutionen bilden eine Gruppe, denn wenn zwei Wege, welche k durchläuft, den Substitutionen S und T entsprechen, wird der Weg, welcher aus diesen beiden zusammengesetzt ist, der Substitution T S entsprechen. Diese Gruppe heisst die *Monodromiegruppe* der Gleichung mit Beziehung auf k. Dieselbe möge mit H bezeichnet werden.

221. *Die Substitutionen der Gruppe H verändern nicht den Werth einer monodromen Function von k.* Jede der Substitutionen wird nämlich ausgeführt, indem man k den derselben entsprechenden Weg durchlaufen lässt; da die Function monodrom ist, erhält sie indessen immer denselben Werth, sobald k zu seinem ursprünglichen Werthe zurückkehrt, ohne Rücksicht auf den durchlaufenen Weg.

Andererseits *muss eine Function monodrom sein, sobald sie durch alle Substitutionen von H den Werth nicht verändert,* denn diese Substitutionen entsprechen allen möglichen Wegen, welche k durchlaufen kann.

222. *Die Gruppe H ist in der Gruppe G einbegriffen.* Alle Substitutionen von H lassen nämlich den Werth einer jeden rationalen Function unverändert, da eine rationale Function von den Wurzeln und k auch monodrom ist.

Dagegen wird H in der Regel nicht alle Substitutionen von G enthalten, denn es ist nicht nothwendig, dass eine Function, weil sie monodrom ist, rational durch bekannte Grössen ausgedrückt werden kann. Sie kann z. B. gewisse numerische Wurzelgrössen enthalten, und wird erst dann rational ausgedrückt werden können, wenn man diese adjungirt. Erst diese Adjungirung wird dann G auf H reduciren.

223. *Die Gruppe H ist mit allen Substitutionen von G permutabel.*

Es sei ψ eine Function der Wurzeln, deren Werth nicht durch die Substitutionen von H, wohl aber durch alle übrigen Substitutionen verändert werde. Dieselbe ist dann eine monodrome Function von k und kann also als eine rationale Function von k mit gewissen irrationalen Coefficienten ausgedrückt werden. Diese Coefficienten mögen durch a, b, c... bezeichnet werden; dann setze man den Ausdruck in die irreductible Gleichung ein, welche zur Bestimmung von ψ dient. Man erhält dann gewisse Gleichungen zwischen a, b, c..., welche ausdrücken, dass der Bestimmungsgleichung für alle Werthe von k genügt wird. Man kann dann eine solche Gleichung bilden, dass a, b, c... rational durch eine ihrer Wurzeln ausgedrückt werden (74). Adjungirt man die Wurzeln dieser Gleichung, so wird G auf eine Gruppe reducirt, welche keine Substitutionen enthalten kann, die nicht in H vorkommen. Diese Gruppe muss dann eben H sein, denn H kann durch Adjungirung von Zahlenwerthen nicht reducirt werden. H ist deshalb mit den Substitutionen von G permutabel (202).

224. Als Beispiel möge die Gleichung betrachtet werden, welche $\cos\frac{z}{n}$ durch $k = \cos z$ bestimmt. Die Wurzeln mögen durch $x_1, x_2 \ldots x_n$ bezeichnet werden, wo $x_p = \cos\frac{x + 2p\pi}{n}$. Ausser $\cos z$ adjungire man $\sin z$. Aendert z sich continuirlich,